The End of Secrecy?

Military Competitiveness in the Age of Transparency

Beth M. Kasper, USAF

August 2001

23

Occasional Paper No. 23
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01AUG2001	N/A	-

Title and Subtitle The End of Secrecy? Military Competitiveness in the Age of Transparency	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Kasper, Beth M.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Air War College Air University Maxwell AFB, AL	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 68	

The End of Secrecy?
Military Competitiveness in the Age of Transparency

by
Beth M. Kaspar, Lt Col USAF

August 2001
Occasional Paper No. 23
Center for Strategy and Technology
Air War College

Air University
Maxwell AFB, AL

The End of Secrecy?
Military Competitiveness in the Age if Transparency

Beth M. Kaspar, Lt Col USAF

August 2001

The Occasional Papers series was established by the Center for Strategy and Technology as a forum for research on topics that reflect long-term strategic thinking about technology and its implications for U.S. national security. Copies of No. 23 in this series are available from the Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, AL 36112. The phone number is (334) 953-6150.

Occasional Paper No. 23
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base, Alabama 36112

Contents

Figures

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

About the Author

Lieutenant Colonel Beth M. Kaspar, USAF, is a career member of the USAF acquisition corps. She began her career as an acquisition logistics officer assigned to Electronic Systems Division, Boston, Massachusetts, where she supported the Joint Tactical Information Distribution System engineering development, Have Quick Radio production, and an experimental combat identification system until 1985. She was then assigned to Rome Laboratory, Rome, New York, where she was the principal investigator for Advanced AWACS sensors and passive surveillance applied technology development and the advocate for Rome Laboratory POM development and execution. In 1989, she was reassigned to the Pentagon as the Program Element Monitor for USAF avionics and C3I science and technology programs within the Pentagon. Following intermediate service school in 1993, Lieutenant Colonel Kaspar joined the Defense Advanced Research Projects Agency where she was the program manager for four guidance and targeting research programs with an annual budget in excess of $40 million per year. Lieutenant Colonel Kaspar is a graduate from the Armed Forces Staff College, Defense Systems Management College, a distinguished graduate from the Air Command and Staff College and Squadron Officers School. She has a Bachelor of Engineering Degree in Electrical Engineering from South Dakota State University, and a Masters of Science Degree in Engineering Management from Western New England College.

Preface

This study focuses on military competitiveness in the age of transparency, and asserts that the U.S. military must consciously prepare itself to fight in an information transparent world created by globalization. The worldwide explosion in the quantity and quality of information and products available to the general public user, the ready accessibility to the information, and the affordability in acquiring any desired data or product is creating a transparent world at an alarming rate. In the future, anyone can affordably keep tabs on the actions of everyone else. Hence, the U.S. military must consciously begin to investigate ways to maintain its military advantage in this rapidly evolving, and increasingly transparent world. It must minimize the impact transparency has on how we will fight wars and conduct contingency actions. We must not be caught by surprise. Maintaining U.S. military competitiveness will require multifaceted solutions.

My sincere thanks to Dr.. Grant Hammond and Col. (Ret) Theodore Hailes of the Air War College's Center for Strategy and Technology (CSAT) for giving me the opportunity to conduct this research. Thanks also to Mr. Ted Kluz, Dr.. Joseph Aein, Col. (Ret) Dr.. Randy Gressang, and Col. (Ret) Joe Bianco for taking the time to challenge the thesis, debate these issues, and provide invaluable advice regarding this study.

Abstract

Information and communications technologies are having a profound impact, both domestically and globally, on how future war will be waged. These technologies are providing affordable, worldwide, near real-time, 24-hour, CNN-like news coverage; worldwide Internet access; and more importantly, access to commercial space systems, including remote sensing, communications and navigation. Unfortunately, this explosion in world-wide information and communication systems creates vulnerabilities for U.S. national security. One such vulnerability is information transparency. This transparency is the result of the worldwide explosion in quantity and quality of information available to the general user, the accessibility to this information, and the affordability in acquiring any data product desired. The resultant electronic information symmetry makes the world transparent, where anyone can keep tabs on the actions of everyone else.

This study investigates how the U.S. can retain its military advantage in the coming age of transparency. The inevitable economic pressure of the "web," or more generally information e-commerce, is advancing the rate of global transparency. Relying only on the National Command Authority to continue with its approach of controlling information release to the public is doomed. Transparency can seriously degrade several principles of war, most significantly mass, maneuver, and surprise. For example, it will provide an adversary near-real time, accurate battle-space visibility of U.S. military posture at both the strategic and theater levels. As such, an adversary could preemptively deny forward basing by destroying air bases or sea ports, use his own long range precision strike weapons against pre-selected U.S. targets, and selectively deny U.S.-developed space based navigation to counter surprise attacks. In essence, transparency affects military capability - for both sides - in temporal and spatial dimensions.

U.S. military planners must accept that information transparency is inevitable and proceed to minimize its affects on our military capability. Deliberate innovation in doctrine, advanced weapon systems, and organizational structures must be initiated to mitigate the speed and clarity, or celerity that information transparency provides. Only by being prepared, can the U.S. maintain its competitive military edge.

Chapter 1
Introduction

Rapidly emerging information and communications technologies are going to profoundly impact how future war will be waged. The increasing availability of high-quality commercial satellite-based communications, navigation, and surveillance information; ready access to the Internet or other worldwide computer networks; and twenty-four-hour worldwide media coverage to virtually anyone who wants it may be a great equalizer in future conflicts. No longer can nation states control information released to the general public and the rest of the world. Because of the irrevocable, accelerating progress of information sciences and economic globalization, information "e-commerce" is advancing at exponential rates. In the future, virtually anyone will be able to play. Unfortunately, denying or delaying access to "bad actors" may be difficult or impossible technically, politically, and legally.[1]

To deal with these threats, the U.S. national command authority (NCA) must consider a more deliberate approach to unleashing offensive weapons in space. As the world's last remaining superpower, the international community will not see the use of space weapons as justifiable unless there are compelling reasons. However, some experts even question whether such weapons would be effective given that new satellite systems are less vulnerable to disruption because software automatically reroutes traffic when a satellite goes down.[2]

Since it is reasonable that the U.S. military could face a condition of "information transparency" in which anyone can keep tabs on the actions of others, this study investigates steps that will help the U.S. military remain competitive in an age of transparency. It begins by examining transparency as a result of the explosion in affordable, robust commercial satellite services; rapid evolution in dual use technology; and expanding demand for continuous worldwide news coverage.[3] This study then explores how this emerging transparency will influence U.S. military capabilities because it will undermine several principles of war, most notably mass, maneuver, and surprise. The study also considers how

transparency could affect the ability of the United States to fight as part of a coalition or use technology as a force multiplier. Last, this study examines possible steps the U.S. military can take to mitigate the effects of transparency. Since information transparency is inevitable, the U.S. military must develop superior capabilities, which will depend on using doctrine, organization, and procurement to counter the effects of global transparency.

Chapter 2

Shifting Secrecy

> *"Global dominance will be achieved by those that most clearly understand the role of information and the power of knowledge that flows from it."*
>
> Adm. David E. Jeremiah
> Former Vice Chairman, Joint Chiefs of Staff

In April 1986, Moscow squelched rumors of a leak of nuclear by-products at its Chernobyl nuclear facility, but U.S. government satellites captured an unobstructed view of the damaged power plant. Only twenty-four hours after the Pentagon analysts first saw the wreckage, ABC News broadcast the same view obtained from a commercial satellite. The pictures were blurry, but the underlying message was clear.[4] The age of total government monopoly on high-tech surveillance was over.

Increasingly, information technologies that were once the exclusive purview of the governments of the United States and the Soviet Union are available commercially for purchase. Spurred by global competition, advances in commercial technology, and a loosening of Cold War restrictions, information-related technologies are available on the open market at affordable prices. High performance computers, satellite imagery, and cryptographic technology are just a few of the traditionally closely held technologies now globally available to individuals or commercial entities. Furthermore, countries can exploit easy access to dual use technologies to develop new systems or modify existing ones such as high performance computers and optical surveillance satellite technology.[5] Another example is a strap-down inertial navigation system for ballistic and cruise missile high-accuracy guidance using computer chips identical to those used in commercial products.[6] Similarly, countries like Iraq can use civilian telephone system compliant to the standards of the International Telecommunications Union, including fiber optic cable, to create a strategic command and control system.

In the following sections, areas contributing to increasing international transparency will be reviewed individually. These areas

include global access to commercial satellite products, high speed Internet access, worldwide, twenty-four-hour media coverage, and dual use technologies. It is important to gain an understanding of the nature of transparency before an assessment can be made on the impact to future war.

Commercial Space

Once the exclusive purview of governments, space technology is rapidly becoming commercial. In fact, commercial firms are investing in space technologies at an unprecedented rate. This year market revenues are expected to top $2 billion, increasing more than six-fold in five years.[7] Several factors contribute to this dramatic growth. Within the last five years we have seen a rapid shift in communications traffic due to the convergence of computer and communications technology. Extraordinary advances in digital signal processing and complex modulation schemes as well as voice and video data compression, have increased effective bandwidth for commercial satellite communications. The second is changes in international space policy, notably deregulating tele-communications services and new frequency spectrum allocations for commercial satellite communications service. The third is the growing dual use aspect of many information technology systems, like the Global Positioning System (GPS), which are finding rapid acceptance around the world. Japan, for example, is the second largest manufacturer of GPS systems after the U.S.[8] Finally, there are fundamental changes in the cost of satellite manufacturing and expanding global demand for satellite services driven by the information revolution.[9] As a result, entrepreneurs are finding commercial satellites and their products to be affordable, reliable, and profitable.

Space-Based Telecommunications. One area that is experiencing significant commercial transformation is satellite-based telecom-munications. As governments, businesses, and individuals around the world seek more information faster, they look to satellites to provide it efficiently and inexpensively. One study predicted global Mobile Satellite Services (MSS) will build on a tremendous growth of services to create a $25 billion market by the year 2004. Subscribers are projected to increase

from 400,000 to 24 million within five years.[10] Furthermore, analyses suggest the annual potential for U.S. global broadband services will grow to nearly $200 billion by 2005 and space-based broadband services will capture fifteen percent of that market.[11]

Major new satellite communications systems are being deployed in the low, medium and traditional geo-stationary earth orbits, or a combination of medium and geo-stationary orbits.[12] The low earth orbit (LEO) systems operate in the 1-2 GHz range and provide voice and data communications, especially mobile telephone service.[13] Proposed systems include Signal (Russian), ICO Global (a seventy-nine nation consortium) and European-African Satellite Telecom (Marconi-Matra). One should note that not all such ventures have been profitable, and recently, the U.S. companies Globalstar and Iridium have filed for bankruptcy protection.

The smaller LEO systems, such as Orbcomm (U.S.) and Starsys (U.S.), operate below 1 GHz and provide data communications such as e-mail, two-way paging, and messaging to remote locations.[14] Broadband LEO systems provide high-speed data services such as video conferencing and Internet access via a Ka-band frequency.[15] Example systems include Teledesic (U.S.), Skybridge (a joint venture by Loral (U.S.) and Alcatel Alsthom), Celestri (European) and Wide-band European Satellite Telecommunications.

In geo-stationary orbit, several new satellite systems are under development including Cyberstar, Spaceway, Astrolink, and Eurosky Way, which will provide global, two-way broadband capability for voice, data, interactive multimedia, and video teleconferencing.[16] A new type of system is the hybrid low and geo-synchronous earth orbiting system, which allows the customer to choose whether a given application is better sent to a low earth orbiting satellite – where near real-time response is desired or a higher geo-synchronous earth orbiting satellite, for applications of a longer duration. For instance, an Internet user could order a video via a low earth orbiter and have the order filled by a higher geo-synchronous satellite.[17] While this market faces extreme competition from the cellular phone industry, it does open up possibilities to governments and militaries around the world to affordably lease space-based transponders.

Increasingly, both industry and the U.S. military rely on leased commercial, primarily geo-synchronous, space communications, such as INMARSAT and PANAMSAT, to provide communications between the U.S. and forward operating locations. In Bosnia, the U.S. military leased a commercial wide-band direct broadcast system to provide reconnaissance data, weather, intelligence on demand, and even Cable News Network to thirty locations at twenty-four megabits a second.[18] This innovative use of commercial communications satellites has fueled the military's appetite for information. The U.S. military already leases space on commercial communications satellites to augment its own resources. Many U.S. Navy warships are equipped with the INMARSAT commercial communication system, allowing voice communications virtually anywhere.[19] The desire for communications connectivity is increasing. In Operation Allied Force in Kosovo, the Allies connected forty different locations in fifteen different countries using a variety of military and civilian lines and satellites.[20] The AF is now evaluating the option of launching dedicated military space-based communications transponders aboard new broadband commercial multimedia systems such as Teledesic LLC and Hughes proposed Spaceway.[21] The Pentagon estimates that by 2008, commercial satellites could carry seventy percent of defense communications and other countries are already moving in this direction.[22] In short, the world is becoming dependent on satellites for business, news, entertainment, international relations, navigation, everyday phone calls as well as military command and control.

Remote Sensing. Space-based commercial remote sensing is evolving along the lines of commercial communications to become a lucrative and viable business. Growing access to higher-resolution satellite imagery has been accelerated by the declassification of U.S. and Russian satellite archives, technological advances in higher resolution sensors for imaging satellites and geographical information systems (GIS), lower launch costs, and growing market demand. What was once the exclusive province of the U.S. and Soviet Union has become available to anyone. The new generation of space-based commercial remote sensing offers any potential enemy similar higher-resolution ground intelligence, at fast revisit rates with rapid distribution at economical prices.

Commercial remote sensing is a dual use technology that has tremendous potential. Industries and governments alike recognize that commercial remote sensing can be an important tool for decision making by supporting such civil applications as weather forecasting, natural resource management, global ecology monitoring, and mapping. It supports commercial applications such as traffic management, pipeline safety, precision agricultural farming, support to media news reporting, and computer games.[23] It also supports a variety of diplomatic/military needs such as peace negotiations, treaty verification, humanitarian operations, as well as military mapping (ten-meter resolution) mission planning, weapon targeting and navigation, and combat operations.[24] Unfortunately, as the Carnegie Endowment asserts, commercial remote sensing can also encourage industrial espionage, terrorism, or more cross-border military attacks in the developing world.[25]

The improving resolution of these space-based commercial remote sensing systems raises concerns. Figure 1 provides a visual comparison of the various resolution levels. Ten-meter resolution is sufficient for *detecting* bridges, buildings, and even concentrations of tanks. Two-meter resolution is sufficient to *generally identify* aircraft, vehicles, roads and bridges while one-meter resolution is sufficient to *precisely identify* types of aircraft, tanks, airport and harbor facilities, cars in railroad yards, vehicles on roads and bridges, and troop units.[26] It is also precise enough to distinguish fighters from bombers or missile launchers from trucks.

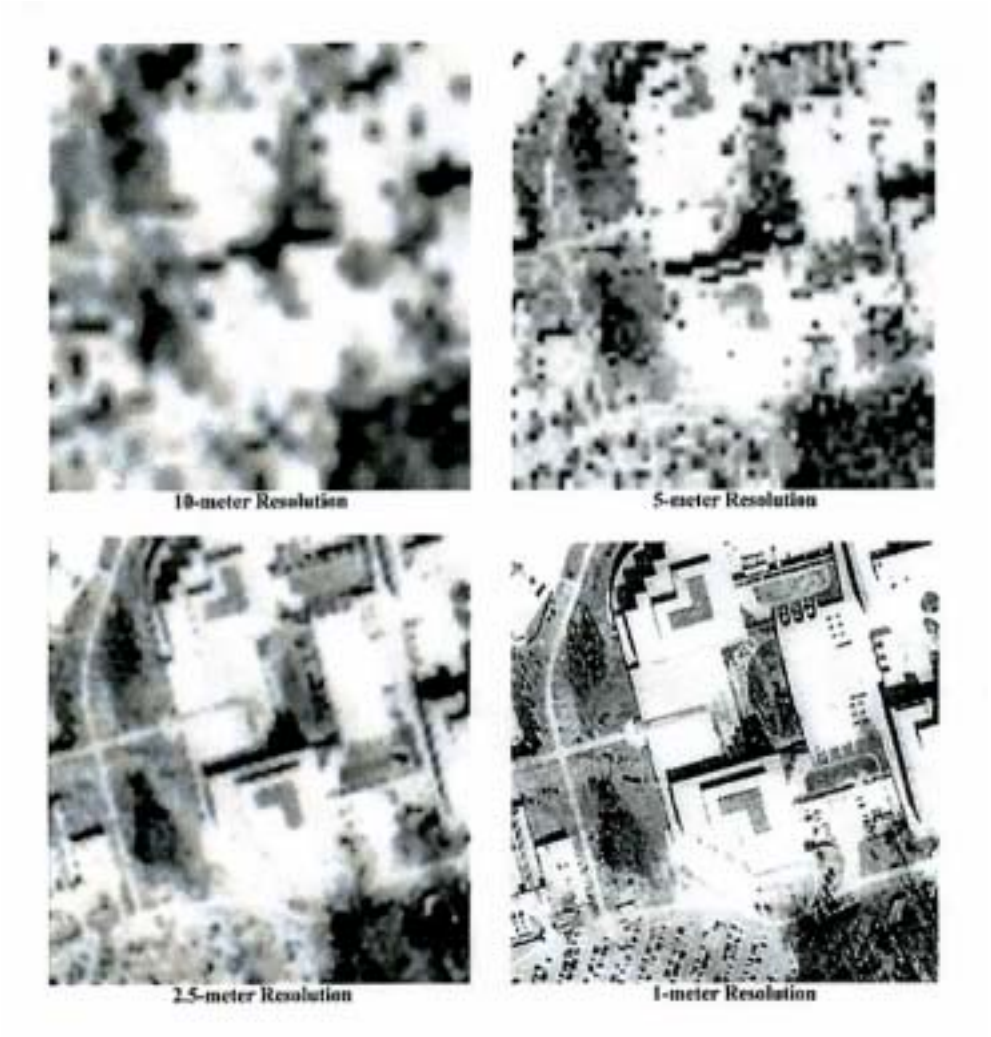

Figure 1 Samples of Commercial Image Resolution

High-resolution satellite images, like those depicted above will soon be readily available from a variety of sources. The U.S. Space Imaging's IKONOS satellite is already providing one-meter (or better) resolution imagery.[27] The U.S. EarthWatch and Orbview companies will likely have launched their one-meter satellites before this paper is published. The Sovinformsputnik Interbranch Association in Russia has been selling two-meter resolution images from its archives using their Sputnik era technology.[28] Duma authorization to sell one-meter images appears

imminent.[29] The West Indian Space Ltd., a joint venture by Israeli Aircraft and California CORE Software Technology, plans to launch one-and-a-half meter resolution EROS satellites by 2002, and South Korea and India plan to launch their one-meter resolution satellites in 2003. [30] Indeed, the projection is that as the number of commercial platforms in orbit soars over the next decade, high-resolution pictures from space will be routinely available, as will cloud piercing radar images and hyper-spectral scans that combine hundreds of light bands to produce intricate details about ground features.[31]

Given the wide range in potential applications, it is not surprising that commercial remote sensing market revenue forecasts range as high as $20 billion per year.[32] Within the next decade, over 100 earth observation satellites may be launched by both private and government entities, and of these, eleven companies in five countries, are expected to launch one-meter resolution satellites.[33] The United States, Russia, France, Israel, India, and South Korea are already developing substantial commercial remote sensing capabilities to take advantage of these applications for national economic development. This new generation of commercial satellites will not only provide imagery data of higher spatial resolution (i.e., one to two meters) but, just as importantly, also offer major improvements in revisit rates, geo-location accuracy, faster distribution, and in some cases stereo images.

Improvements in effective resolution are possible with advanced digital signal processing. France has developed a merged data technique that simultaneously downlinks the imagery taken by the same camera from one satellite via two transmission channels. It then blends two SPOT 5B five-meter resolution images on the ground to produce a two-and-a-half-meter resolution image, which will be available for sale in 2002.[34] It is likely that other commercial satellite companies will develop their own imaging sharpening techniques to create higher resolution stereo images or other unique products for sale. They may even sell the raw images to distributors for data manipulation.

A growing business base in commercial remote sensing is electronic image distribution and processing. Whereas remote sensing once depended on mainframe computers and highly trained dedicated experts, advances in software, data storage, and data processing techniques allow

companies to affordably process the data on desktop computers and easily distribute it in real-time, via CD-ROM and the Internet. For example, using a desktop computer, one can easily geographically reference a large array of data, including the remotely sensed ones, manipulate and analyze it, and deliver the generated information, on time, in the customer's format.

Several start up companies have joined in establishing commercial remote sensing companies in distributing the commercial sensing raw and processed imagery. These companies are usually regional distributors for other nation's satellite company remote imagery. For example, ImStrat Corporation is the U.S. distributor for SPOT imagery, Aerial Imagery of Raleigh, N.C., is the distributor for the Russian two-meter KVR-1000 satellite, and Space Imaging is the North American distributor for India's five-meter resolution IRS family of satellites. In Europe, SPOT Imaging is the distributor for Orbital Sciences Orbview-3 and –4 satellites.[35] Furthermore, several distributors have been given permission to manipulate the raw data to suit customer's needs. For example, ImStrat can merge a one-meter panchromatic image with multi-spectral imagery to produce a product with one-meter special detail colorized with the multi-spectral data.

This trend is creating headaches for the U.S. Commercial satellites will increase the amount of information that can be used against the American forces and allies.[36] But it is not just the volume and clarity of the pictures that is worrisome. The speed of delivery of the picture is becoming a national security problem.

Timeliness of satellite imagery is also dramatically improving. Previously Russian one-meter imagery was unavailable until nine days after it was shot. Now Space Imaging's IKONOS satellite constellation can revisit nearly any spot on Earth every three days at one-meter resolution and daily at lower resolutions.[37] Preliminary images are available only thirty minutes after the shutter snaps.[38] Five-day-old images qualify as archival and sell for between thirty and 300 dollars per square mile of mapped surface on the company's web site.[39] If Space Imaging's two American competitors, Orbital Imaging Corporation and Earthwatch, stay on their launch schedules one-meter visibility will soon be available once each day.[40]

Concern over the improving resolution and timeless of commercial satellite imagery has caused some governments to begin placing controls on remote sensing. U.S. Presidential Decision Directive 23, which was issued in 1994, includes a provision that the U.S. has the right to limit the collection and distribution of high-resolution imagery that might damage national security.[41] This "shutter control" directive applies only to systems licensed for operation in the U.S. France has a similar position as they limit sale of high-resolution imagery from the French owned Helios-1 satellite to friendly governments. Further, they stipulate that the French government can shut down the system in case of national emergency.[42] However, not all nations have similar policies. Israel, for example, is considering launching additional EROS-1 satellites for customer use and giving them total percent control within a specific geographic region.[43] The West Indian Space Ltd., which is a joint U.S. and Israel venture, has no restrictions on the sales of its one-meter images.[44] In the absence of oversight or control, anyone can get a high-resolution satellite image in the commercial marketplace.

The implication is that third party sales can dilute the effectiveness of "shutter control."[45] Unless all the nations that fly imaging satellites enforce similar restrictions, the U.S. will be imposing restrictions while others will be "snapping and selling away." Marketplace forces will rapidly erode the government monopoly on satellite remote sensing and drive U.S. companies out of business because of their inability to compete.

Space-Based Navigation. Another area of satellite development is the U.S. Global Positioning System, or GPS, which has become the global standard for navigation and timing. Developed by the U.S. Air Force over two decades ago to provide precise time and location data to military users, it provided military commanders during the Gulf War with navigation data critical to both moving troops and targeting munitions. Given its success during the War, GPS has been so fully integrated into military operations that by 2002 military planners expect all troops to carry GPS receivers.

More recently, precision guided munitions were used four times more in *Operation Allied Force* than in *Desert Storm* - and that number is constrained only by the limited numbers of precision weapons in U.S. inventory.[46] By 2008, as part of the Joint Direct Attack Munitions (JDAM) program, the AF will have installed GPS guidance kits on nearly

90,000 gravity bombs.[47] Other GPS guided weapons coming in the next ten years include the Joint Stand-Off Weapon (JSOW), modified Conventional Air Launched Cruise Missile (CALCM), Tomahawk Land Attack Missile (TLAM) and new systems such as the Joint Advanced Air to Surface Missile (JAASM) and the Wind Corrected Munitions Dispenser (WCMD).

GPS is irresistible in the commercial marketplace as well. According to the Department of Commerce, the civilian sector has leveraged the Pentagon's $10 billion investment in technology infrastructure into a market for hardware, software, and services that is expected to grow to nearly $16 billion by 2003.[48] In fact, industry observers estimate that military users account for only one-and-a-half percent of the GPS market.[49] GPS is available in automobiles and trucks to aid travelers in navigating unfamiliar streets, to hikers navigating new terrain, to survey and construction crews for precisely locating points, to shipping companies to maintain delivery schedules, to police and emergency medical services to determine the closest source of help for people in need.

The same method it uses to make position measurements also makes GPS an extremely accurate timing system. A new, important dual use GPS application is its intrinsic precise worldwide timing. GPS is the only technology today that can typically provide an accuracy of fifty nanoseconds or greater over intercontinental distances.[50] This is useful in many industries worldwide. It is used in communication systems to synchronize the transmission of cellular phone messages and signals from pager network towers, where a unique time signal tags each call to ensure that it is routed and transmitted properly. GPS timing synchronizes power plant generators to provide electrical phase matching and fault detection throughout power grids in the United States.[51] Investment bankers also use GPS to timestamp trades on international networks to ensure that interest income is calculated properly. This list continues to grow.

The dual use nature of GPS creates problems for the military. First, commercial users are employing local "augmentation" services to provide more accurate location data. They use a base station with a precisely known location, which broadcasts an additional signal to GPS users. This gives the user more accurate position data than even the originally military

encrypted GPS provided. Secondly, GPS is the international navigation standard. In 1996, President Clinton committed the U.S. to provide nonmilitary use of GPS on a continuous, worldwide basis, free of direct-user fees.[52] Although the United States wants to prevent enemy use of GPS during wartime, national U.S. policy dictates the Air Force must operate GPS as a "global information utility" without unduly disrupting or degrading civilian uses of the system. This was reinforced in a recent bilateral cooperation agreement with Japan; the world's other leading producer of GPS equipment.[53]

To the U.S. military, commercial GPS service represents a dangerous diffusion of military capability. After all, GPS is what provides the low cost precision guided missile its accuracy. With this increasing technology diffusion, accuracy may no longer be a U.S. monopoly. According to several studies, potential adversaries could use GPS for cruise missile guidance.[54] In fact, China is already employing a combination of GPS and GLONASS (the Russian navigation equivalent) receivers in an integrated navigation system for their ballistic missiles. The robust combination of GPS/GLONASS improves overall missile accuracy by more than twenty-five percent. As an additional targeting aid, the Chinese are integrating GPS/GLONASS into their mobile launchers to further enhance the initial reference point and increase accuracy.[55] For the U.S. military, GPS is a classic two-edged sword that can be used both for and against us.

National Security considerations may become overwhelmed given the irresistible market forces that are commercializing space. Accordingly, the U.S. military must understand that the products provided by commercial satellite systems, from imagery to communications to navigation, are excellent and cost-effective tools for military organizations. The U.S. military must how this dual use asset will affect its own and other's military capabilities.

Internet: The Information Superhighway

Another key contributor to transparency is the Internet. Within the last five years, Internet traffic has grown eighty-six percent per year, more than six times the growth of voice traffic.[56] In June 1998, Matrix

Information and Directory Services (MIDS) reported that 102 million people are accessing the Internet worldwide and estimates that the total number of worldwide Internet users will grow to 707 million by 2001.[57] Since virtually every country has at least one connection to the Internet, the access to information is unlimited.[58] The only requirement is a personal computer connected to the Internet and one can search massive amounts of information rapidly and systematically for technical and human intelligence information. Figure 2 shows an illustrative, but by no means comprehensive, range of open sources, available software and on-line research services to help people locate anyone or anything.[59]

SOURCES	SOFTWARE	SERVICES
Current Awareness (e.g. Individual Inc.)	Internet Tools (e.g. NetOwl, Web Compass)	Online Search & Retrieval (e.g. NERAC, Burwell Enterprises)
Current Contents (e.g. ISI CC Online)	Data Entry Tools (e.g. Vista, BBN, SRA)	Media Monitoring (e.g. FBIS via NTIS, BBC)
Directories of Experts (e.g. Gale Research, TEL TECH)	Data Retrieval Tools (e.g. RetrievalWare, Calspan)	Document Retrieval (e.g. ISI Genuine Document)
Conference Proceedings (e.g. British Library, CISTI)	Automated Abstracting (e.g. NetOw., DR-LINK)	Human Abstracting (e.g. NFAIS Members)
Commercial Online Sources (e.g. LN, DIALOG, STN, ORBIT)	Automated Translation (e.g. SYSTRAN, SRA NTIS-JV)	Telephone Surveys (e.g. Risa Sacks Associates)
Risk Assessment Reports (e.g. Forecast, Political Risk)	Data Mining & Visualization (e.g. Visible Decisions, TASC Textor)	Private Investigations (e.g. Cognos, Pinkertons, Parvus)
Maps & Charts (e.g. East View Publications)	Desktop Publishing & Communications Tools	Market Research (e.g. SIS, Fuld, Kirk Tyson)
Commerical Imagery (e.g. SPOT, Radarsat, Autometric)	Electronic Security Tools (e.g. SSI, PGP, IBM Crytolopes)	Strategic Forecasting (e.g. Oxford Analytics)

Figure 2 Open Source Niches

These resources can enable one to find virtually anything. For example under the auspices of the Air Force Space Command, a "red cell" was formed to see if it could, using only open-source information and

commercial satellite imagery, track the deployment of an Air Expeditionary Force (AEF) to Bahrain in October 1997.[60] Without any special Internet access privileges, the Red Cell quickly learned a great deal about the AEF deployment, including where the AEF would deploy, its mission, and its force composition. The team tasked the French SPOT satellite to image the AEF bed-down locations in Bahrain, as well as Mountain Home Air Force Base, Idaho.[61] Analysts located the AEF headquarters, hardened aircraft shelters, refueling areas, and housing for deployed personnel.[62] In this way, the Red Cell created a valuable intelligence picture using open source Internet references and commercial satellite imagery.

Further, the Internet can distribute this or any information to anyone, including those with little experience with search engines. With a Pentium-class PC, a graphics program, image processing software, and an Internet connection, anyone anywhere can buy and manipulate high-resolution imagery for an investment less than $10,000.[63]

The Internet can also be used to hide information from an adversary. If you don't want a satellite to see what you are doing, you can determine when satellites will be passing overhead and then deceive or deny the satellite sensors the correct information. For example, it was reported that personnel at the Indian Nuclear Testing Grounds were moved out of view to avoid being seen during passes by U.S. satellites. As a result, the U.S. was surprised when India tested their nuclear weapons in May 1998.[64]

In addition to gaining access to satellite data, the Internet can be used to find trained photo interpreters to extract valuable intelligence date from overhead imagery. A brief search on the Internet revealed at least twenty different individuals and companies advertising imagery analysis services. There are at least one on-line aerial photo interpretation tutorial and numerous catalog extracts for university-level photo interpretation courses.

The Internet provides more militarily useful information than just satellite imagery. The web offers many sites that will provide specific military items like camouflage and concealment netting. Companies, like Barracuda, develop frequency-reflecting camouflage nets to hide objects such as tanks and armored personnel carriers from satellites. Complicating matters further, recent web technology advancements allow

for the concealment of an individuals' Internet addresses. Montreal Canada Zero-Knowledge Systems Inc has launched a new service that lets people remain completely anonymous while sending e-mail, visiting Web sites, or making purchases over the web.[65] It allows individuals to hide not only identities but also their Internet trail.

The Internet is a "super-library", open to all, twenty-four hours a day with essentially no restrictions. Its impact is being magnified as it combines with wealth of readily available information through twenty-four-hour information news networks.

Worldwide Media Coverage

Continuous news coverage can provide potential adversaries highly accurate military assessments more rapidly than that provided by traditional military intelligence analysis. In open societies, such as the United States, the reasons behind U.S. actions and the types of actions being taken are increasingly discussed in public and the media. The result is that military secrecy is becoming increasingly rare.

Traditionally, the media is obligated to protect vital military secrecy while seeking out stories to fulfill the "people's right to know." However, the competitive pressures to have the most recent news will be exacerbated as commercial satellite imagery and knowledgeable consultants are increasingly available. In 1999, during a Columbia University Seminar on Media and Society, ABC News Anchorman Peter Jennings and CBS News Anchorman Mike Wallace were challenged on a moral dilemma of reporting the news or saving American soldier's lives. After agonizing, Peter Jennings said he would withhold the story while Mike Wallace said he would report the news saying, "There is no higher calling."[66]

The revealing of military secrets is a particularly challenging issue. The proliferation of "all news" networks like the Cable News Network (CNN), Skynews, and others impact political and military actions. CNN reporting of the infamous "Highway of Death" was followed closely by the decision to end the war, which should serve as a reminder of the effects of public information on war. Another example is the sharp reduction of coalition air strikes against leadership targets after the

destruction of the Al Firdos bunker in the fourth week of the Persian Gulf War. Coalition target planners had no prior indication (before seeing post-strike television coverage over CNN) that civilians had occupied this legitimate military target.[67] After the report, General Schwarzkopf implemented a policy wherein he personally reviewed any target selected for air attacks in downtown Baghdad. Those images decisively altered our operational and strategic goals.[68]

Decision-makers increasingly consider not only actual media coverage of events such as air attacks on Iraqi's trying to flee the Kuwait Theater, but also *anticipate* coverage of such events.[69] One report suggested the Cable News Network (CNN) had more pertinent information than CIA Intelligence Estimates in terms of its impact on White House decision making.[70] Continuous news is significant because it represents information that is immediately available to the public. Furthermore, the convergence of near-real time commercial imagery and leased commercial communications satellites with twenty-four-hour news media increases access to critical information. [71]

The globalization of information means that media organizations can use information technologies to influence a nation's political and military agenda.[72] Known as the "CNN effect," global, real-time news coverage makes the conduct of military operations open to immediate public scrutiny.[73] The military's rapid pullout from Somalia may be attributed to the CNN effect. The American government was compelled to reassess its policy when CNN and others broadcast powerful images of a naked dead Marine being dragged through the streets of Mogadishu, Somalia. Additionally, continuous coverage news organizations transmit significant intelligence information when they broadcast real-time satellite imagery of U.S. deployments or coalition actions as occurred when the U.S. Marines landed at Mogadishu and the coalition strike aircraft departed from Aviano Air Base, Italy during Operation Allied Force. Adversaries could mine the Internet for data and news media for intentions, create hypotheses, and then use commercial satellite imagery to evaluate and access possible U.S. courses of action. As a result, Internet access, competitive space-based remote sensing, and twenty-four-news coverage are all converging to make it exponentially harder for military operations to be kept secret.

In conclusion, the transparency of military information is inevitable. It is the result of worldwide economic globalization, the dual use nature of new technologies and the shift of new technology development from military to commercial organizations. The explosive advancements in commercial remote-sensing, navigation and communications space systems, Internet access and powerful Internet web search engines and access, and global coverage of continuous news all point towards the evolving age of transparency. This diffusion will impact the nature of war. The U.S. military needs to recognize this trend and asset its impacts.

Chapter 3

Transparency and the American Ways of War

> *Our enemies have seen CNN. They watched the technology and they will not be content to fight the son of DESERT STORM. They will fight the stepson of Chechnya, the stepson of Allied Force in Kosovo.*
>
> General Charles Krulak
> United States Marine Corp

As the result of the globalization of our economy, our open society, and the evolving dual use nature of military and commercial technology, the U.S. military veil of secrecy is disappearing. The explosive advancements in commercial space systems with remote sensing, telecommunications, and navigation, Internet access, and global coverage is creating a transparent world. The challenge to the U.S. now is to assess how future military operations will be impacted by this transparency and create effective responses.

Throughout the history of conflict, military leaders have associated certain principles with military victory. Known as the cornerstone of military thinking, these principles of war are considered universally true and relevant.[74] The first U.S. exposition on the "principles of war" appeared in the War Department Training Regulations Number 10-5 of 1921. Since then few changes have been made to the nine-item list, which today includes the principles of: objective, offensive, mass, economy of force, security, surprise, simplicity, maneuver, and unity of command.

The U.S. military has been integrating information technologies into its operations for the last ten years so that it now depends on computers, computer networks, and high-speed communications.[75] The implication is that the possession and manipulation of information itself is a critical element of warfare. While information manipulation via ruses, stratagems, and deception has always been a part of warfare, the increasing diffusion of information means information itself is now both a weapon or target.[76]

This chapter will investigate how information transparency is changing the American ways of war. It will begin by first investigating the impact transparency has on the nine principles of warfare. It then shifts perspective and look at how transparency impacts U.S. preferences for coalition warfare and the use of technology as a force multiplier.

Impact on the Principles of War

Principle of War #1 - Objective. "Direct every military operation towards a clearly defined, decisive and obtainable objective that contributes to strategic, operational, or tactical aims."[77] In application, this principle refers to the unity of effort, directing all efforts to achieving a common goal. From an airman's perspective, this principle shapes priorities to allow air and space forces to concentrate on military priorities. It also seeks to avoid diverting force elements to support fragmented objectives. Information technology serves as an enabler for obtaining better-defined, clearer objectives. The clarity and speed at which the data is provided to the appropriate military organizations creates the demand for more information and fewer communications delays so that commanders do not have to wait for critical information. Transparency may negate this "waiting-for-more-data" delay syndrome as commercial sources may provide some critical information.

However, transparency may work against the U.S. military because commercial tools used are likely to be available to our adversaries. They may benefit from commercial communication and remote imaging satellites, Internet access with associated data mining technologies, and continuous news reporting. From this, potential adversaries can garner information about U.S. military troop locations, equipment deployments, and political and military objectives from interviews of U.S. officials and "expert guest" commentaries. This can then be added to other open source information on railroad traffic and ship movement, air traffic control, and spare parts orders to discern U.S. objectives. The adversary could then use this data to develop countervailing strategies to various possible U.S. courses of action.

Principle of War #2 - Offensive. "Seize, retain and exploit the initiative. Dictate the time, place, purpose, scope, intensity, and pace of operations: Act rather than react."[78] For aerospace forces this means to control the air and space, while to information warriors, this means to control the flow of information and achieve information dominance. Since transparency makes it more difficult to achieve surprise and select targets, the challenge for the United States is to attain the initiative when an enemy could monitor U.S. actions with commercial information systems. For example, in a regional conflict an adversary could detect the initial deployment and initiate immediate actions to offset the attack. Furthermore, judicious uses of deception and denial techniques would make it difficult for U.S. target analysts to develop robust target folders. In effect, transparency increases the need to maintain secrecy, but it involves far more than just tactics.

One observer has asserted that American forces were stalemated in Korea, defeated in Vietnam, and humiliated in Lebanon and Somalia when their opponents *took* the strategic initiative and forced the kind of fight where high firepower and air power could not be used effectively.[79] The French experience in Indochina and the Soviet experience in Afghanistan were similar.[80] In each case, the adversaries chose not to fight "western style" but rather in their own cultural styles.

In the age of increasing transparency and political desire to minimize casualties and entangling conflicts, a competent adversary could seek to deliberately mislead information systems to create a strategic vulnerability for the U.S.[81] This may involve deception and camouflage in order to overwhelm U.S. information collection systems with wrong or misleading information. Another approach would be to limit the effectiveness of collection systems by using redundant fiber optic systems for national command and control, which would be more difficult for the U.S. military to destroy. The overall effect would be to make it more difficult for U.S. forces to prosecute the war, which is troublesome when the U.S. military uses information technology to offset the declining size of the military. Any U.S. strategy that fails to anticipate the problems caused by transparency will create strategic vulnerabilities for the nation

Principle of War #3 - Mass. "Concentrate combat power at a decisive time and place."[82] For airpower, the principle of massed forces has changed

by precision weapons, because aircraft no longer have to fly in mass formations to strike a target. Today, with superior information and targeting capabilities, one aircraft with one precision-guided weapon can destroy a target that in an earlier age might have required hundreds of bombs. As a result, campaign plans have become carefully orchestrated events designed to support the weapon releaser. Strike packages, composed of escort jammers, stealth and conventional fighters and bombers, and tanker escort, supported by theater surveillance and communications systems, must all be tightly choreographed and synchronized together to perform their specific function, at the designated time, for the overall strike mission to be effective. If the planning fails, aircraft/pilots are at risk of being shot down.

Transparency will redefine military planning because adversaries can determine where U.S. forces are originating from and where they will mass. For example, they may use their own high revisit rate satellite imagery or Internet purchased commercial imagery to evaluate U.S. forward basing locations and activity. They could use commercially purchased night vision equipment to detect night attacks, and position GPS jammers near high value targets to degrade the effectiveness of U.S. precision munitions.

However, the U.S. can respond in various ways to these developments. Since the U.S. military can use fewer sorties and precision munitions to achieve the desired effect, it may not be necessary or desirable for the U.S. to mass as many platforms over the objective. In addition, strike aircraft could synchronize theater-wide strikes from a large number of small bases. Finally, the U.S. could reorganize its planning, tactics, and logistics to disperse combat power over the attack zone in order to mask its real purposes.

Enemy Example: Deny U.S. access to theater. Two preconditions that enable U.S. forces to possess the strategic agility, overseas presence, power projection, and decisive force capabilities essential to defeat aggression are adequate time to deploy U.S. forces overseas and unobstructed access to theater seaports and airfields. If either is degraded or denied by an enemy, U.S. national military strategy would be less effective. It is likely that intelligent enemies will use diplomatic,

economic, military, and political instruments of national power to delay, disrupt, or block U.S. forces from deploying into theater.

In Desert Storm, Americans and potential future adversaries learned that it takes a long time to deploy large numbers of forces (ships, planes, and troops) to a theater of conflict. In the future, the time to deploy forces overseas will have critical consequences. The longer it takes for the U.S. to decide whether and how it will engage, the more advantageous it will be for an adversary. Department of Defense studies state that U.S. forces must have at least two weeks of actionable warning and uninterrupted deployment time. If the warning and deployment time is less than two weeks, or if the adversary starts shooting before U.S. forces are fully deployed and in place, significant military risk results.[83]

The implication is that future adversaries will use information transparency. As a result, the assumption in many classic wargames, that U.S. forces have unlimited and unobstructed access to theater ports, airfields, and coastal waters is highly questionable. It is conceivable that in future actions, because of an adversary's coercive diplomacy, the U.S. could lose access to forward bases, be denied over-flight rights, or accept restrictions on how the overseas bases may be used. This could have tremendous implications for military operations. For example, aircraft might have to operate from greater distances, which involves additional time to strike targets, and may increase the size of the support packages needed to get the strike aircraft to their targets. This, in turn, could increase the number of aircrews, maintenance, and support personnel stationed forward to maintain air operations. The implication is that an adversary could reduce sortie rates and the number of bombs dropped on targets while exposing U.S. forces to greater risk, thus undermining the ability to fight the short, low casualty war the U.S. prefers. Even worse, geography and diplomacy by an adversary can severely constrain U.S. actions. For example, in 1996 U.S. led forces ended up watching helplessly when Iraqi Republican Guards invaded the UN declared safe haven Kurdish city of Irbil, located about 200 miles north of Baghdad. When Turkey, Jordan and Saudi Arabia decided they would not allow air strikes against Iraq to be launched from within their territories, U.S. options were significantly narrowed. Unable to strike the offending Iraqi Republican Guards in Irbil, the U.S. was forced to strike air defense

facilities south of Baghdad with forces that were within range of the target. [84] Coalition sensitivities to the U.S. plan created significant obstacles.

Adversaries could also exploit commercial satellite imagery, communications, and the media to influence U.S. or host nation decision-makers and retard the military decision cycle and tempo of U.S. military operations. They could launch precision- guided missiles using conventional, biological or chemical warheads against airfields and seaports. The enemy could determine when best to launch a strike by data mining the Internet, exploiting commercial imagery to determine movements and monitoring the news media to obtain strategic warning and track U.S. deployments. These tactics could be used to punish any country granting U.S. access to its facilities, and to prevent U.S. basing and resupply.

Massive disruption of this sort is not novel. In 1943 a German air strike against Allied shipping in the harbor of Bari, Italy demonstrated that weapons of mass destruction (WMD) can have decisive effects against seaports. More than thirty ships had choked the harbor waiting to unload, among them the USS John Harvey, which was loaded with 2,000 chemical bombs, each with sixty to seventy pounds of mustard gas. Within twenty minutes 105 JU-88 German bombers sank seventeen ships and caused several tankers to explode. When the John Harvey was hit, its mustard gas began to burn. Much of it spread throughout the harbor mixing with the tons of oil floating on the water. A mustard gas cloud formed and killed over 1000 people. The port was closed for three weeks and its operational capacity not resumed for two months.[85]

This event could be replicated today with poison gas or a petroleum spill that shuts down a major port area. If adversaries wanted to limit U.S. access to a theater of operations, a country supporting the U.S. could find itself faced with sea mines, submarines, and attacks against its ports and airfields. In short, degrading U.S. power projection capability is not that difficult. All an adversary has to do is make the price of access too high for the U.S. and its coalition partners to continue.

Accordingly, it is sensible for the U.S. military to modify its power projection strategy when an enemy armed with relatively inexpensive weapons, including cruise and ballistic missile, could devastate aircraft

parked on unprotected flight lines that are located only several hundred miles from the battle zone. In the case of the U.S. Air Force, it might be prudent to develop new aircraft protection measures, such as distributed basing and employment of underground shelters that are used by many other countries.[86]

Principle of War #4 - Surprise. "Strike the enemy at a time, place, or in a manner for which the enemy is not prepared."[87] It is one of air and space power's strongest advantages. Concealing one's capabilities and intentions creates the opportunity to strike the enemy when he is unaware or unprepared. However, the transparency created by the proliferation of dual use technologies, modern commercial satellite surveillance technology and warning systems, Internet, and media coverage, can make it increasingly difficult for the U.S. to mask or cloak any large-scale marshaling or movement of personnel and equipment. Since transparency may seriously jeopardize the military's ability to achieve strategic or tactical surprise, or worse make surprise highly unlikely, the U.S. military may have to change its methods for achieving surprise.[88]

At the same time, transparency also negates tactical surprise, which raises questions about how the U.S. can move or place forces on alert in secret. The increasing reliance on the guard and reserve units makes this even more difficult. Further, naval assets are easily tracked, as are troop and aircraft movements of virtually any scale. When one adds the increasing dependence on contractors for battlefield support, U.S. troop deployments and movements can be easily monitored. Given these conditions, surprise will become an increasingly elusive commodity for the U.S. unless new procedures and methods are developed.

Principle of War #5 - Maneuver. "Place the enemy in a position of disadvantage through the flexible application of combat power."[89] The ability to integrate a force quickly and to strike directly at an adversary's strategic center of gravity is a crucial advantage of air and space power. It requires the flexibility, responsiveness, and clarity that information systems provide to support determination of the maneuver plan. Having near-instantaneous situation understanding confers a decided advantage that must be immediately exploited to be of tactical or operational benefit.

But with transparency, this can work to the advantage of either friend or foe when each player knows what the other is doing. For example, the smaller U.S. Army of today could not accomplish the "left hook" that it conducted during *Operation Desert Storm* given the proliferation of space satellite imaging systems. U.S. naval units are similarly unable to hide in the vastness of the oceans given the information capabilities that currently exist.[90]

By this standard, the Persian Gulf War was the last secret war rather than the first open modern war because, as reported in the Gulf War Air Power Survey, this may gave been the last war in which only one side had ready access to precise location information from satellites.[91] The implication is that information transparency is becoming a fact of life with which the U.S. military must deal.

Principle of War #6 - Security. "Protect friendly forces and their operations from enemy action. Never permit the enemy to acquire an unexpected advantage."[92] In the modern era, there are four areas that must be protected which are critical to how the United States conducts military operations: airpower on the ground (i.e., at airbases), space system ground control elements and telecommunication links to the satellites, logistics facilities, and command facilities including information centers. With the increased dependence on information for battlespace dominance, each pathway that carries intelligence, command information, or relevant data must be protected from being intercepted, tapped or disrupted. But given transparency, this is becoming more difficult.

Just as it was possible to use information from the Internet to track the movement of the Air Expeditionary Force in 1997, so an adversary could use commercial information to track U.S. ship or convoy movements, debarkation and embarkation areas, staging and bed-down arrangements. Alternatively, an adversary could use commercial data base management and data mining technologies to track and target military activities. Since the "pizza index," the number of pizzas delivered to the Pentagon, has been flagged as an accurate predictor of future U.S. military operations, an adversary could track sharp rises in deliveries and use commercial satellite imagery to track Pentagon parking lot occupancy during U.S. combat deployment planning and execution. In order to conceal operations,

information security will be more difficult and must cover a broader base of indicators.

The diffusion of information could clearly limit the U.S.'s ability to project military power and adequately protect forward bases, particularly if opponents are equally well informed of events in a campaign. An adversary could use the Internet to estimate possible U.S. deployment areas, computing gateways or communications and control centers, airbases, or seaports. It could then launch a surprise attack, disperse assets, set out decoys to deliberately confuse overhead and theater sensors, destroy coalition forward operating bases with tactical missiles, live off pre-distributed supplies in protected locations, and if the U.S. or coalition counter-attacks, force a non-western style of war. As General Fogelman, former U.S. Air Force Chief of Staff, said, "It would make it extremely costly to project U.S. forces in to a disputed region, much less carry out operations to defeat a well-armed aggressor. Simply the threat of such an enemy missile attacks might deter the U.S. and coalition partners from responding to aggression in the first instance."[93]

It is hard to exactly predict the impact of such a response on the pace of U.S. operations, but U.S. actions could be significantly delayed, disrupted, and degraded. China knows this. They now have seventeen spy satellites and forty domestic satellites to continuously track and monitor the global movements of the U.S. military. These satellites could easily be used to guide a "saturated" missile attack on American and Taiwan warships.[94] China is also entering into commercial satellite imaging contracts with non-U.S. space companies and in joint ventures with other countries to develop an indigenous capability to either launch satellites alone or jointly with others.[95] China could use these new capabilities to pose a significant threat the U.S. ability to project military power. It is conceivable that with long-range cruise missiles and robust satellite surveillance, China, could inflict heavy losses on U.S. land-based and naval forces.[96]

An adversary could also selectively degrade theater GPS and communications support. For example, a strategic center of gravity of the coalition forces in the Gulf War was their heavy dependence on the orbiting U.S. navigation and communications satellites. If Iraq had destroyed the Defense Satellite Communication System (DSCS), the allied

advantage would have been weakened.[97] The U.S. military's dependence on GPS and communications satellites has increased since then. During the war against Serbia, GPS was essential for guiding precision bombs to their targets in bad weather, maneuvering ships, and positioning troops. This makes U.S. satellite based communication and navigation systems even more lucrative targets for adversaries than in years past.

To neutralize the GPS signal broadcast from space, an adversary could use local jammers to degrade GPS and commercial satellites, as well as terrorist attack ground stations.[98] China, for example, could seek to prevent the U.S. from using its leased commercial communications satellites and supporting ground stations in Asia. The implication is that there are many ways for interrupting satellite signals. Without navigation satellites, the U.S. would lose its timing and positioning system for targeting munitions, and without communications satellites, the United States would have difficulties commanding its military forces.

An adversary's ability to use one-meter resolution satellite imagery and CNN expert consultants discussing U.S. deployments may not be the final arbiter of success. The adversary must have the weapon systems and personnel to make full use of the information. From the U.S. perspective in this evolving era of transparency, our weapon system capability and training in tactics and decision making may make the difference. The quality of people and platforms and the fast-breaking ability to innovate and adapt in combat – at all levels – will be a major factor in future conflicts.

Principles of War # 7-9 – Simplicity, Unity of Command and Economy of Force: The three remaining principles of war, namely simplicity, unity of command and economy of force are not directly impacted by transparency, but these principles influence how the United States might negate the effects of transparency.

Simplicity. "Prepare clear, uncomplicated plans and concise orders: avoid unnecessary complexity in organizing, preparing, planning, and conducting military operations." The impact of transparency depends on whether the commander is a micro manager. Those who micromanage every aspect of the operation will, of necessity, create deception plans of great complexity, negating the principle of simplicity. On the other hand,

if the commander is strictly task oriented, and leaves the details up to subordinate commanders, transparency will have little impact on simplicity.

Unity of Command. "Direct and coordinate all efforts towards a common objective."[99] Unity of command is important for all forces, but it is vital in employing air and space forces. While it ensures that one commander is responsible, it is unknown whether one commander can manage all of the information. Information technology enables commanders to fax, email or video teleconference consult with one another or coalition partners or senior political leadership in near real-time. If this transparency supports both sides equally, then the critical factor will be who can make better decisions in the shortest time.

Economy of Force. "Employ all combat power available in the most effective way possible; allocate minimum essential combat power to secondary effort.[100] Optimum economy of force requires a complete awareness of the tactical situation. At the same time, the U.S. military is becoming increasingly dependent on information exploitation so that it can employ just the right amount of combat power at the right place at the right time. However, this reliance creates vulnerabilities. For example, there were reports in *Operation Allied Force* that NATO dropped over 3,000 precision-guided weapons, but hit 500 decoys and destroyed only fifty Yugoslav tanks. This is significant because early in the war NATO and U.S. stocks of precision weaponry were low. The concept of economy of force was jeopardized because of Serbian information denial techniques, such as camouflage, effectively used information transparency to its advantage.

In short, the U.S. Military's Principles of War are general guidelines for how to employ force and conduct military operations. From this brief review of the principles of war it is seen transparency affects all of the principles of war to some degree – the most serious being mass, security, and surprise. In essence, proliferation of technology globally is changing the science and art of war.

Transparency - a Technology Equalizer

Besides the long established, guiding principles for war, the U.S. has two other historical preferences for waging war. One of which is that the U.S. has been a strong technology proponent, arguing that technology is a force multiplier against numerically superior forces.

This tremendous faith in technology is an abiding American characteristic. The idea that superior technology can be leveraged to make up for shortfalls in numbers of troops, weapons, or dollars, is both appealing and traditional.[101] Since the beginning of the Cold War, the U.S. has historically relied on technology to provide superior firepower against numerically larger enemy forces. The U.S. military uses its superior technology as an asymmetrical tool for conducting warfare.

For example, in the Gulf War the U.S. exploited its available technology to achieve military dominance. It used laser guided bombs with night-capable target acquisition and tracking devices; sophisticated night-capable tank fire control systems; long range precision strike cruise missiles, widespread secure voice communications and facsimile machines for command, control and coordination; beyond-visual-range air-to-air weaponry; and airborne radar systems such as Joint Surveillance Target and Reconnaissance System (JSTARS), which monitored the land battle in detail.[102] Another force multiplier for U.S. forces in the Gulf War was information exploitation.[103] National surveillance and reconnaissance, missile-launch warning, navigation, and leased commercial communications assets were all used to ensure successful coalition operations. More recently in Bosnia and Kosovo operations, the U.S. exploited technology advantages in GPS, precision target acquisition and track systems, and miniature missile navigation and guidance systems to achieve standoff, surgical strikes.

While these technologies were successful against inferior adversaries, their success was offset by unanticipated difficulties. Difficulties arose in applying our intelligence systems and analytical methods, controlling the swift operational tempo of the war, and achieving effectiveness given the asymmetrical response by the adversary.

As transparency increases, unanticipated difficulties will increase, and the technological advantage the United States has always assumed it will have, will erode away. Because of the diffusion of dual use technologies, many others are starting to share in this force multiplier technology. Therefore in a sense, the U.S. military needs to reexamine the basics. In the future, how the military adapts its doctrine and culture to new technologies may be more important than the science and technology itself. Further, as unintended difficulties arise with using these new technologies, a key to success will be rapid adaptation.

Impact on Coalition Warfare

The U.S. has fought most 20th Century modern wars as a member of a coalition.[104] Since the end of the Cold War, coalitions have been an increasing factor in dealing with collective threats. The 2000 U.S. National Security Strategy speaks to the U.S. commitment to remain engaged overseas and work with allies to create international structures strengthening security and prosperity.[105] The underlying National Military Strategy asserts the U.S. will fight future wars as part of a coalition or alliance.[106]

Coalition (or alliance) warfare adds another element of friction to the already unpredictable and chaotic events of war. Over the last fifty years in NATO, the U.S. has sought to minimize the chaos by mandating standardized equipment and interoperability. However, the air war over Serbia highlighted significant problems, including the failure to maintain a Euro-Atlantic interoperability baseline. The use of three different generations of aircraft and equipment created difficulties that spanned interoperability, command and control, and mission planning.[107] This wide gap between the U.S. and NATO countries has caused considerable unease on both sides of the Atlantic.

Coalition fighting will only become more difficult as the technology gap with our friends widens while the technology gap with our potential adversaries closes. As NATO Secretary-General George Robertson said, "Today technology is moving so fast that some of NATO's members are in danger of being left behind."[108] Unfortunately, Allied members have not and are not making the investments in their military defense structure

to keep up with U.S. advances. European nations as a whole spend less than half of that of the U.S. on procurement and a third of its research-and-development budget on defense.[109] Furthermore, European and U.S. critics alike contend that the money European governments do devote to the military is not well spent.[110] Therefore because of the risk that transparency may level capabilities with adversaries but widening the gap with traditional allies, the Atlantic-Euro partnership must create a new concept of coalition operations. Maintaining a stance of integrated coalition operations maybe politically correct, but if European investment in military forces does not improve, it could become militarily unexecutable.

Transparency may also exacerbate tensions in coalition politics and cause problems for military operations. Transparency requires fast, focused decision making, but coalitions typically have slow, broad-based decision processes. During Operation Allied Force, Secretary of Defense William S. Cohen learned first hand how slow coalition decision making could be. He remarked, "It became clear quite quickly that NATO needed to retool its existing political machinery to be more effective for what I would call the staccato timing of a military contingency."[111] Nineteen countries wanted some oversight of how military operations would be conducted. Political leaders became deeply involved in day-to-day targeting decisions and individual countries would veto both individual missions and whole classes of targets. This oversight slowed the targeting cycle greatly, which, had NATO faced an adversary able to capitalize on transparency, would have placed the alliance at a significant disadvantage.

Globalization, military competitiveness, and transparency mean that everyone, including our potential adversaries, have relatively rapid access to evolving technologies. The U.S. must therefore continue to advance its military capability to protect U.S. interests. Since the U.S. cannot underwrite the modernization costs of our European alliance or coalition forces, it finds itself at a defining point of what coalition and alliance warfare means in the Twenty-first Century. Things must change. The enemy will not be sitting still while the U.S. struggles to shape its alliances or coalitions into cohesive efficient military tools of policy.

Chapter 4

Implications to U.S. Military Competitiveness

> *Sometimes, looking straight ahead – even with the most dedicated attention and seasoned experience – just misses both the big picture and the new ideas, because they often come at you from "left field." Ironically, the more successful that you are, the more likely that you'll miss those seeming orthogonal ideas. Success can be your worst enemy.*
>
> Nicholas Negroponte
> Cambridge Massachusetts

A central question is how transparency may affect the nature and conduct of war. During the Gulf War, the U.S. was able to exploit information for the purpose of achieving dominance in military operations by linking electronic warfare, intelligence, surveillance, and target acquisition with the use of precision-guided munitions from air, land, and sea platforms simultaneously. This required the seamless integration of information, which is now a requirement for the U.S. military and a vulnerability adversaries may exploit in future conflicts.[112] At the same time, the U.S. military must adapt to the transparency caused by technological diffusion if it is to remain a military superpower, which will demand organizational and doctrinal innovation.

Doctrinal Innovation

Despite its military accomplishments in the Persian Gulf War and its continued incorporation of information technologies into the military, the United States must consider the second and third-order effects of employing new weapons on military doctrine. An important first step is to rethink *Joint Vision 2020* strategy, which established a framework for joint warfare in the future. This strategy rests exploiting information systems and satellites to achieve information dominance, which allows U.S. commanders to detect enemy forces, maneuver and fire with greater effectiveness, and use military logistics support with greater efficiency.[113]

However, with the rapid diffusion of information technologies, many states will be able to operate more effectively on the battlefield.

One option for the United States is to accelerate decision making. This is essentially upgrading John Boyd's "Observe-Orient-Decision-Act (OODA) loop into what Dr. Grant Hammond calls the "OODA point."[114] Therefore, technology and doctrine must be integrated so that connectivity is more important than distance. By the year 2020, the U.S. military will be able to conduct air, naval, and ground operations at faster rates over longer distances. Since it is impractical to prepare for all contingencies, military organizations must develop the ability to deal rapidly with all types of contingencies. With the emphasis on using technological solutions to fight future wars, it is essential for the U.S. military, particularly given events in Kosovo, Bosnia, and Somalia, to rethink doctrine.

The simultaneity of employing overwhelming combat power throughout the breadth and depth of an operational area requires our information exploitation systems and connectivity to be better than an adversary's. It also requires a new mindset away from linear battlefields and controlled decision making. The U.S. military should strategize and practice how this non-linearity would work, train for reduced decision making time, and modify weapon system equipment acquisitions for extreme modularity to best exploit this rapidly evolving transparent global world.

Escalation Strategy and Doctrine: Related to this is the need to develop strategies and doctrine that gives political authorities the ability to escalate violence within conflicts while maintaining control over the political objectives. NATO's *Operation Allied Force* in Kosovo underscored the Clausewitzian dictum, "The political objective is the goal, war is the means of reaching it, and the means can never be considered in isolation from their purpose."[115] Kosovo was a place where the total war mentality did not correspond to the coalition's political objectives.

The recent NATO conducted Operation Allied Force in Kosovo underscores the need for a new "less than total war" mentality. NATO's Supreme Allied Commander believed the only way to prosecute the Kosovo war was to go for the first-round knockout by hitting the Serb troops hard right from the start. He wanted to avoid a quagmire like

Vietnam where the military was too cautious and the politicians too restrictive. General Clark believed NATO should win 'twenty-one to nothing.' However, there were some who preferred to win by a score of seven to six.[116] The overwhelming night attacks were viewed as excessive, and due to his failure to understand the political realities that underscored the war, in July 1999, General Clark was notified of his retirement.[117]

Since then, General Clark has been reexamining the sequence of events that led to the war, and has concluded that there may be a better way to handle such conflicts in the future. In November 1999, he stunned the U.S. Senate Armed Services Committee when he called for a complete rethink of Western strategy and he questioned the need for the aerial assault on Serbia. General Clark noted that NATO could have used legal means to block the Danube and the Adriatic ports, and could have used "methods to isolate Milosevic and his political parties *electronically*."[118] If implemented and augmented with other measures, Clark added; *the military instrument might have never been used*.[119] Others in NATO concur.

At the recent NATO conference in Brussels on Kosovo, Sir Michael Alexander, chairman of the Royal United Services Institute for Defense Studies in London, argued for the development of an escalation strategy. "Anyone who believes multinational coalitions or gradual escalation won't be a part of NATO's future is fooling themselves. In democracies," he said, "gradual escalation is the name of the game, because the only circumstances in which our governments could talk of the ground force option is when the horrors of the ground really began to impact on public opinion to the extent that the politicians felt they could get away with it. That is going to be the case in the future."[120]

With the increasing need to contain small-scale conflicts, the U.S. military must develop effective joint strategies and doctrine to fulfill the America's need to escalate conflicts or coerce without conducting overwhelming parallel warfare. Given the U.S. military's experiences in Kosovo, today's "hot spot" global climate, and the lessons of Vietnam, it seems realistic for U.S. military to add this capability to their arsenal.

Coalition Operations. Operation Allied Force demonstrated that coalition decision making is untimely and ineffective. While the U.S. and

allied equipment has become increasingly incompatible during the last decade, coalition forces will be interoperable and effective only if their capabilities are designed to interface with those of the United States. The U.S. must apply its scientific and technical strengths to develop multi-level security systems that allow coalition partners to connect with U.S. systems. This way, the U.S. can maintain its revolution in military affairs while establishing downward compatibility with established alliances and future coalition partners.

Coalition consensus decision-making is too slow. In the age of transparency, this is unacceptable. Therefore the U.S. must help NATO learn to react inside the enemies decision loop. The U.S. must lead NATO in developing a new command and control structure that maintains coalition unity but reacts more quickly. The DOD must consider various methods to speed up or focus the coalition decision process – even at risk of some loss in security.

Camouflage, Concealment & Deception. From the use of the Trojan horse to Serbian mockups that look like tanks, deception has stymied more powerful armies. For example, the U.S. used mockups of tanks and landing craft prior to the invasion at Normandy in 1944 to convince German aerial reconnaissance into believing the attack would be at Calais. China and Russia routinely use camouflage, deception, dispersal, mobility, and secrecy to limit an adversary's information, and in fact, Russians taught the Iraqis and Serbians how to use deception. It is now time for the U.S. military to incorporate deception into all organizations and plans for war.

Commercial Technologies. Since technology is critical to the evolution of military doctrine, the United States must use commercial technologies more effectively. To do this, the U.S. military must use experiments and wargames to test commercially available technologies and new concepts, and to develop new strategies and doctrine. Without such efforts, the military may be increasingly insulated from emerging technologies and real-world capabilities. In the future, the U.S. military will need a flexible and adaptive force posture with sufficiently large and diverse assets as well as an effective doctrine and planning framework to ensure success in future military operations.

Selected Technology Development to Counter Transparency Effects

Since, technology is constantly advancing, the military must invest heavily to ensure it maintains its technological edge, and then use this technology to innovate constantly in order to stay ahead. However, there are limits to what technology can accomplish as demonstrated by the U.S. operation in Somalia in 1993, the inconclusive aerial attacks against Iraq in the late 1990s, the fate of the Albanian Kosovars in the NATO air war against Serbia in 1999, and the vulnerabilities to missiles and terrorism that modern societies face.[121]

Despite these limits, potential adversaries who are less technologically and economically capable than the United States, are benefiting directly from global information transparency. As a result, the United States will need to define new military concepts to address this. To that end, the following technological ideas may be useful.

Data Analysis and Interpretation. The Chairman of the Joint Chiefs of Staff, General Henry H. Shelton, recently noted "information operations and information superiority are at the core of military innovation and our vision for the future of joint warfare. The capability to penetrate, manipulate, and deny an adversary's battlespace awareness is of utmost importance."[122] However, the operation in Kosovo exposed problems with this concept because, despite NATO's near total information superiority, the Serbian military manipulated NATO's battlespace awareness. For example, strikes on fake targets indicate that either the Serbs let NATO daytime reconnaissance flights see real targets and replaced these at night with decoys, or that U.S. target analysts misinterpreted the digital data provided them. The implication is the Serbs developed low-technology responses that misled NATO intelligence systems and limited NATO's information superiority advantage.

These errors wasted expensive munitions. Hitting the right target on time requires sorting out the proper coordinates from extraordinary amounts of information. It is time to challenge the scientific community to quickly and correctly sort through and interpret the tremendous amounts of information generated in modern wars. The U.S. military needs to develop techniques that lead to improvements in battlefield visualization,

language translation and cultural identifiers, and analysis of the methods and sources used to interpret data.[123] Until we can improve the analysis of the overwhelming inflow if data, intelligence and targeting analysis will continue to be a critical weakness.

Decision-Making Processes. Since success in future military operations could depend on adapting to rapid changes on the battlefield, the U.S. military must use its advantages in information processing to make decisions much faster. During *Operation Allied Force*, NATO could not process information quickly enough to enable aircraft to strike mobile targets, in part because of the reaction time that was required to pass data from EC-130 (airborne command, control, and communications) aircraft to NATO's Combined Air Operations Center in Vincenza, Italy, and then to strike aircraft.[124] It is time to deliberately improve the process so that the intelligence system can manage information in real-time and handle dense waves of data.[125] We must refine the "observe, orient, decide, act, or "OODA loop," into an "OODA point." As Mr. Keith Hall testified to the Senate Armed Forces Services Committee this spring following regarding Kosovo, "We have to find ways to collapse that cycle of collection management tasking, collection processing exploitation, and dissemination, and move it from what has been past, days, or at least hours, to minutes."[126] Furthermore, decision-makers must be trained to use the information systems and their experience so that they can make those risky decisions rapidly and continuously, which ultimately depends on using systems able to process more information in less time.

This capability will require state of the art commercial imagery equipment, multi-media indexing technology, and real-time distribution systems to get the right information to the right person on the first try. Since the U.S. military is likely to be engaged in relatively small-scale regional conflicts where leadership, cultural symbols and political motivation are critical key factors, it is essential to develop methodologies and processes to identify valid information in near real time.

A related issue is the exploitation of unmanned air vehicles (UAVs).[127] UAVs provide an important surveillance and reconnaissance capability. They can gather targeting and intelligence data at low altitudes, under poor weather conditions, and at night in order to feed targeting and reconnaissance systems. Often, this is data that space-based

and higher altitude sensor systems cannot gather or cannot provide with sufficient real-time flexibility and resolution. Unless the observe and orient phases of the OODA process are based on valid information, we will end up with misinformed decisions and inappropriate actions.

Lastly, we must create flexibility in our "act" phase so that we can immediately responsive to unfolding military situations. The creation of a "dynamic ATO process" would allow command centers to update targeting information while aircraft or missiles are still in flight, which will permit them to use new information to alter the overall course of the campaign.[128] This can be accomplished by directly linking mission planning and air control systems to the strike aircraft so they can change missions in real-time regardless of the number of allied aircraft in the theater of operations.

Sensors. The U.S. has increased its reliance on remote sensors so that it can conduct pinpoint attacks with weapons launched at long-distances from targets. Because most fielded U.S. sensors can't see inside things or distinguish between a decoy covered in metallic foil and the real thing, the likelihood exists that our commanders will not always have the confidence to act decisively. [129] In the recent Kosovo conflict, Serbia used wood and plastic sheeting, metal tape, and metal plates to build phony targets of mockup tanks, armored personnel carriers and other ground decoys. As a result, the U.S. must develop the technology and methodology that will allow military commanders to detect concealed and mobile targets, and distinguish the real targets from mockups. This capability may be based on image fusion of infrared, panchromatic, and other sensors that are geo-spatially coordinated to verify a target's actual composition, and speedily forward that information to the attacking pilots. In the Kosovo example above, radar alone might present a confusing picture, but a combination of infrared sensors, which could detect if an engine had been used recently, and signal intelligence to determine whether there were normal communication patterns among tanks, would make it vastly more difficult to use decoys.[130]

Fiber Breaking Weapons. If the U.S. is serious about degrading the enemy's command and control infrastructure, it must upgrade its munitions. Using fiber optic cables for transmitting information continues to proliferate at an accelerating rate as more countries and companies

deploy Internet transmission facilities. For example, the company Global Crossing notes that by the end of 2000, their network will include access to eighty percent of the world's major traffic routes.[131] Other companies, like Project Oxygen are competing to provide any customer with high speed, high connectivity fiber optic routing worldwide.

Yet as mentioned earlier, these fiber optic based advanced networks are particularly tough to destroy with precision-guided munitions.[132] In the Gulf War against Iraq and again during Operation Allied Force, in the Balkans in 1999 against Serbia, there were serious problems in attacking the command, control and communications systems. Reportedly, Iraq and Serbia had made extensive use of commercial telephone switching networks and multiple buried fiber optic cables.[133] These facilities are militarily difficult to degrade yet quickly repaired with redundant connectivity. The U.S. military must develop the capability to successfully destroy this form of communication, as this destruction will be a fundamental requirement in future conflicts.

Adapt the Organization

While improvements in doctrine and technology are necessary for the U.S. to remain a preeminent military power, they are not sufficient. Future conflicts will require military organizations to continuously adapt to survive. Given the erosion of U.S. advantages by global transparency, the winner of the next war will be the side that can best execute and adapt their strategy to the war at hand.[134] Therefore, the U.S. must inculcate into all levels the dual use of information – information as a tool and as a weapon – for both sides. To do this, several actions are required.

Maintain Quality Force. Quality is a relative thing, and much depends on the quality of the adversary's forces. But given the increasing proliferation of technology around the world, the U.S. military must not only equip its forces with the most advanced technology, but must also continue to recruit and train high-quality personnel. This is more important than ever because poor skills create vulnerabilities in the form of mistakes that even an enemy with lesser technology can exploit. Furthermore, with poor skill levels it will be impossible to conduct

sophisticated tactics and operational routines to get the most out of the new systems coming on line.

As it is now, maintaining a highly skilled quality force is difficult. The volunteer force influenced by a host of factors including low salaries, availability of civilian employment, high operational tempo, and potential for casualties. Over the past several years, these factors together have made maintaining a quality force difficult. A more robust retention program with selective bonuses or professional pay for people in high technology specialties is required. Keeping computer programmers, photo analysts, and other transparency negating skills is critical for today's military, and with increasing transparency, this will be even more important in the future.

Knowledge Operations. The Gulf War demonstrated unambiguously the value of achieving information dominance in military operations. The U.S. Armed Forces used 188 mobile ground stations and twelve commercial satellite terminals to process satellite communications during the war. Linkages to U.S. databases and networks were complex – up to 700,000 telephone calls and 152,000 messages were handled every day. In order to conduct the forty-two-day air war, more than 30 million telephone calls were necessary.[135] The combination of database management systems and airborne and satellite sensor system fusion permitted theater air commanders to implement the campaign strategy with appropriate mission execution.

In the future, the U.S. must not only protect our information-based systems, it must also validate information to protect against undetected adversarial data manipulation. Many of our systems are vulnerable. For example, over seventy percent of U.S. military communications are carried commercially with security being almost non-existent at most commercial satellite operations centers. With these vulnerabilities, the U.S. military must assume that the adversary will seek to radically improve their decision-making cycles and degrade those of the United States. New arrangements to bolster security in the commercial sector may be needed. Such arrangements may require Civil Reserve Air Fleet like funding and use contracts.

Further, the military must make use of information in ways that accelerate the decision cycle. As transparency speeds an adversary's

decision processes, the U.S. military will need to increase its decision speed to maintain an advantage. In short, the U.S. military must inculcate into its thinking that data is a modern weapon.

"Overloaded" Decision-Making. One of the most interesting and underrated lessons learned from the NATO operations over Kosovo was that "information superiority overload can actually hurt mission performance."[136] When people where overwhelmed by too much information, they could not focus on the right information.[137] This problem extended to video teleconferencing as well, since it can become a "voracious consumer of leadership and key staff working hours."[138]

If we are to remain superior in the age of information transparency, the U.S. military must establish mechanisms to teach its future leaders how to deal with information overload or information chaos. This training must be conducted across all levels: strategic, operational, and tactical. While not a total solution, Professional Military Education sponsored war game simulations and real-time computer based exercises would likely be beneficial. Anything that would teach its future leaders how to make intuitive decisions under pressure with an overwhelming but incomplete data set is a step in the right direction towards successful combat in the age of transparency.

Forward Basing. The U.S. Air Force needs to rethink where and how establishes bases in theaters of operations to protect aircraft and people. A recent RAND report warns that an enemy armed with cheap versions of cruise missiles or ballistic missiles could devastate aircraft parked on unprotected flight lines when the bases are a few hundred miles from the battle zone.[139] Therefore, the Air Force should take actions to minimize its footprint near and around the combat theaters.

One concept that may be useful is distributed mini-basing. This concept uses a number of forward operating locations to enhance expeditionary operations. These forward operating locations may be as Spartan as a dirt strip for C-130s, or an unobstructed section of highway reinforced with polyurethane folded mats. The use of alternative locations to disperse aircraft will make each base less lucrative as a target for terrorists or potential adversaries. [140] Combat operations would use a theater-wide system to plan and adjust events in real time so that participating strike aircraft, originating from geographically dispersed

areas, mass as strike packages over the combat zone. To support future expeditionary air force operations, the U.S. Air Force must address the effects of a small number of overseas and collocated operating bases in an age of information transparency, which may mean expanding the numbers of airfields that can be used for expeditionary purposes.

Realistic Wargames. It is essential for the U.S. military to conduct realistic war games and exercises, which deal with the problems caused by corrupting or jamming communications links as well as degrading GPS data. U.S. military forces must learn to manage the inevitable problem associated with information that is corrupted or unavailable as a result of enemy action. At the same time, the Department of Defense should re-establish a separate "RED TEAM" organization within the Joint Chiefs of Staff, evaluate the vulnerabilities that are being created by information transparency. In short, wargames where victory is preordained and the victory party scheduled before the game even begins, need to be replaced by realistic exercises where the "good guys" might actually lose.

Chapter 5

Conclusion

> *The only constant in our business is that everything is changing. We have to take advantage of change and not let it take advantage of us. We have to be ahead of the game.*
>
> Michael Dell
> Dell Computer Corporation

The appearance of the written word, a few millenia before the invention of the printing press in the Seventeenth Century, transformed military power. It enabled the preparation and dissemination of complex orders and the delegation and coordination of operational and tactical command functions and organizing logistics. As a result, larger armed forces could be mobilized, logistically supported, and deployed effectively in combat. Extended operations by larger forces made command and control even more important, a trend that continued with the advent of the telegraph, telephone, and radio. Today's exponential growth in the microchip's computing power, the availability and affordability of high-speed information technologies, and global proliferation of networked public information centers enhance the ability to gather, analyze, and disseminate data and enables its manipulation via real-time movement of electronic words and images. The desire for more information to reduce the fog of war remains unabated with the advent of information technologies.[141]

Today's information revolution is analogous to the written word revolution. It is the catalyst for economic, political and military change on a global scale. Economic globalization and commercial technology diffusion is making the world more transparent, where anyone can know the business of anyone else. As the technology diffuses, so to potentially does the U.S. military technological lead.

Despite our efforts to restrict the rate of technology transfer, commercially based information technology is rapidly and irreversibly proliferating around the world. As foreign militaries incorporate information technology and public data sources into their doctrines and

tactics, transparency has the potential to seriously erode our position of dominance unless U.S. forces plan for and use this transparency to their advantage. Chinese strategists argue that the United States overestimates its ability to achieve information superiority with a determined adversary who has a well-established program to deny accurate information to U.S. sensors. They give two reasons for this position. The first is that, because of its gratifying experience in the Gulf War, the U.S. military has become complacent and reluctant to part from its existing military force structure and concepts. Consequentially, future enemies can use this conservatism and evolving information transparency to revolutionize their military capabilities by using more advanced thinking than the U.S.[142] The second reason is that the proliferation of information technology is eroding the U.S. superiority in information dominance. To a great extent, some of the world's most advanced technology is widely available on the commercial market. Chinese strategists point out that the U.S. overestimates its ability to gain information superiority in the face of a determined adversary who has a well-established program to deny accurate information to U.S. sensors.[143] The diffusion of technology, which is integral to global transparency, increases the chances that states could impede, if not deny, the ability of the United States to project military power.

There has been a failure to consider how information transparency might erode U.S. information superiority and thereby reshape the principles of warfare that guided its military strategy during the Twentieth Century. If the enemy can use transparency to see U.S. actions in near real time, the principles of mass, security, surprise, and to a lesser degree maneuver, objective, and offensive are harder to achieve. If bases and seaports are more vulnerable to enemy attack, the only choice may be to disperse forces in order to keep them safe from enemy attack, which could influence the principles of unity of command, economy of force, and simplicity.

Information transparency could affect how the United States uses technology to maintain its military competitiveness. Because transparency levels the abilities of many states, the United States should seek to maintain its technological advantage by developing a strategy for exploiting transparency and increasing its ability to fight and win wars. This will involve investigating the possible consequences of transparency

on military doctrine, modernization, and organization. In terms of doctrine, the U.S. military must reconsider whether it is properly positioned to meet the goals of *Joint Vision 2020* for using information as a weapon.

In addition, the military also must use camouflage, deception, and denial to prevent potential adversaries from using information as a weapon against the United States. This will involve improving its sensors to deal with concealment, developing weapons that destroy fiber optic networks, and creating tools that will help intelligence analysts identify targets. Additionally, the U.S. military must revamp its organizational structure in order to create a smaller and less noticeable footprint in the theater. Finally, it is essential to help military commanders make the right decision when operating under great pressure an in the presence of massive amounts of information. In essence, the United States must examine how information transparency could influence its national military strategy.

This is a compelling age in history. The exponential growth in globally marketed information systems with dual use technologies and products is creating a transparent world. But this transparency has ramifications on both how the U.S. military will fight and how it will prepare to fight. If the U.S. military wants to maintain its competitive position, it must evolve doctrine, acquire superior weapons and systems, and adapt a viable organizational structure. If we fail in this, commercial technology diffusion and advances will outstrip doctrinal and weapon system developments with potentially devastating consequences. After all, as the Roman General said, "He who desires peace, let him prepare for war."[144] The time to prepare is now.

Appendix A
List of Available Internet Sites

Satellite Imagery

Focal Point Graphics at http://208.228.111.128/avhrr.html

Microsoft's TerraServer at http://www.terraserverr.microsoft.com

Earth Observation Data Services at http://www.observe.de/geoids/geoshop.cfm

SPOT Imagery at http://www.spot.com

Satellite Image Interpretation

Pinpoint Geographics Inc. at: http://pinpointgeographics.com/index.html

Sereda Engineering Co. at: http://enviroenterprise.com/sereda/html

Fleximage at: http://fleximage.fr/indexa.htm

Notes

1. Buchan, Glenn, "Information War and the Air Force: Wave of the Future? Current Fad?" Issue Paper, RAND, March 1996.

2. Crock, Stan, "Space: The Final Battleground?" *Business Week*, 15 June 98, Issue 3582, p. 122.

3. In the past, many of the DOD science and technology achievements, designed to maintain a technologically superior military force, have progressed to the civilian economy and formed the basis of technological advancement in industry. Today, there is much movement of technology in the other direction, from the commercial world to defense.

4. Florini, Ann., "The End of Secrecy", *Foreign Policy*, Summer 98, Issue 111, p. 63.

5. Carus, W. Seth, "Military Technology and the Arms Trade: Changes and their Impact," *Annuals of the American Academy of Political and Social Science*, Sep 94, Vol. 535, p. 169.

6. Ibid., p. 167

7. Peters, Katherine McIntire, "Space Wars", *Government Executive*, April 98, Vol. 30, Issue 4, p. 13.

8. Johnson, Dana J. and Scott Pace, and C. Bryan Gabbard, *Space: Emerging Options for National Power*, RAND, 1998, p. 37.

9. Moorman, General Thomas S., USAF Retired, "The Explosion of Commercial Space and the Implications for National Security," *Airpower Journal*, Spring 99, Vol. 13, Issue 1, p. 6-21.

10. Lantz, Terry D., Mobile Satellite Services", http://doserve.mall.nsa.ic.gov/producer/ttn/8-2/mobile.html

11. See 1998 Booz-Allen and Hamilton consulting firm analysis available at http://www.tcmet.com/tcmet/newsit/H1000249.htm

12. Ibid.

13. Johnson, Dana J. and Scott Pace, and C. Bryan Gabbard, *Space: Emerging Options for National Power*, RAND, 1998, pp. 25.

14. Ibid, p. 25.

15. Ibid, p. 25.

16. Moorman, S. (Gen), "The Explosion of Commercial Space and the Implications for National Security", *Airpower Journal*, Spring 99, vol. 13, Issue 1, p. 10.

17. Lantz, Terry D., "Mobile Satellite Services," Oct 25, 1999, http://doserve.mall.nsa.ic.gov/producer/ttn/8-2/mobile.html

18. Black, J. Todd, "Commercial Satellites: Future Threats or Allies?" http://www.nwc.navy.mil/press/Review/1999/winter/art5-w99.htm

19. Fuller, Andy, "Inmarsat Maritime Services and Products," Inmarsat Facts, January 1997, http://www.inmarsat.org/inmarsat/html/media_supp/factsheets/maritime.pdf.

20. Myers, Richard B (Gen), Investment in Space, *Air Force Magazine, February 2000,* p. 51.

21. Ibid. p. 24.

22. As a rule, countries (besides the U.S., Russia, and UK) that wish to have a military presence in space will usually opt for dual-use satellites, which carry both military and commercial transponders. Ibid, p. 25.

23. Television companies like CBS regularly use two-meter resolution imagery in news bulletins. Red Lemon, a Glasglow, Ireland computer game manufacturer, used Russian developed satellite mapping of Scotland for its most recent game, Braveheart.

24. Tahu, George J. and John C. Baker, "Expanding Global Access to Civilian and Commercial Remote Sensing Data," *Space Policy*, Aug 98, Vol. 14, Issue 3, p. 188.

25. "Eyes in the Sky a Growing Concern," http://www.space.com, 17 Mar 2000, pp. 20.

26. Policy Makers not ready for Commercial Imagery," Defense News, Issue XX, April 3, 2000, p.1.

27. Verton, Daniel and L. Scott Tillett, "Commercial Imagery Prompts NIMA Doubts," *Federal Computer Week*, Oct 18, 1999. Also at http://www.fcw.com/pubs/fcw/1999/1018/fcw-newsnima-10-18-99.html.

28. Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999.

29. Anselmo, Joseph C., "Commercial Space's Sharp New Image," *Aviation Space and Week,* Vol. 152, No. 5, January 31,2000, p 56.

30. Israeli EROS (previously a military system, now commercial) boasts a one-meter resolution in some applications. The stated goal for the next launch is 1.5-meter resolution. "Eros Partners Will Modify Ground Stations for Free," Space News, February 18, 1997. See also http://www.coresw.com/news/sn19970218.html

31 Ibid.p.122.

32. Tahu, George J. and John C. Baker, "Expanding Global Access to Civilian and Commercial Remote Sensing Data," *Space Policy*, Aug 98, Vol. 14, Issue 3, p. 179.

33. "Policy Makers not ready for Commercial Imagery," Defense News, Issue XX, April 3, 2000, p.1. See Also "Eyes in the Sky a Growing Concern," at http://www.space.com, 17 Mar 2000, p. 19.

34. "SPOT 5 Improvements Reflect Policy Shift," *Space News*, February 12, 1997. See also http:www.coresw.com/news/sn19970212.html

35. Amato, Ivan, "God's Eyes for Sale," Mar/Apr 99, Vol. 102, Issue 2, pp. 36.

36. "U.S. Officials See Pros and Cons in New Imaging Satellites," *Space News*, 7 Nov 99.

37. Crawley, James W., "Satellite is looking at you, kid," *The Arizona Republic Newspaper*, pp. E1.

38. Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999. See also http://delphi.dia.ic.gov/admin/EARLYBIRD/990907/s19990907private.html.

39. Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999. See also http://delphi.dia.ic.gov/admin/EARLYBIRD/990907/s19990907private.html.

40. Ibid.

41. The White House, Office of the Press Secretary, "Statement by the Press Secretary," 10 March 1994. Also at http://library.whitehouse.gov/Search/Query-PressRelease.html.

42. Gupta, Vipin, "New Satellite Images for Sale," *International Security,* Summer 1995, p. 94.

43. Ibid., p. 104.

44. Wright, Robert, "Private Eyes," *New York Times Magazine*, Sept 5, 1999.

45. Foreman, Tom, " Satellites are Watching You," ABC World News Tonight, Jan 17, 2000. See also www.abcnews.go.com/onair/WorldNewsTonight/ wnt_000113_CL_satellites_features.html

46. Cordsesman, Anthony H., "*The Lessons and Non-Lessons of the Air and Missile Campaign in Kosovo",* Center for Strategic and International Studies, Sept 29, 1999, pp 21.

47. Newman, Richard J., "The New Space Race," *U.S. News and World Report*, November 8, 1999, p. 36.

48. Martello, Norman, "Where in the World," *Electric Perspectives*, Mar/Apr 99, Vol. 24, Issue 2, p. 14

49. GPS Industry Council, 1996

50. Martello, Norman, "Where in the World," *Electric Perspectives*, Mar/Apr 99, Vol. 24, Issue 2, p. 16.

51. Ibid. p. 18.

52. Fact Sheet, the White House, Office of Science and Technology Policy and National Security Council, subject: U.S. Global Positioning System Policy, 29 March 1996.

53. The White House, Office of the Press Secretary, "Joint Statement by the Government of the United States of America and the Government of Japan on Cooperation in the Use of the Global Positioning System," 16 September 1998.

54. Sewell, Kelly, "Sensor Integration Placing GPS Devices on Center Stage," *Military & Aerospace Electronics*, May 96, Vol. 7, Issue 5, p. 25.

55. Stokes, Mark A., *China's Strategic Modernization: Implications for the United States,* Strategic Studies Institute, September 1999, p. 92.

56. Global Crossing Fact Sheet. http://globalcrossing.com/network.asp

57. Ibid, www.mids.org/mmq/501/pub/ed.html

58. Ibid

59. Matthews, Lloyd J., "Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?" U.S. Army War College, 1999, pp. 158.

60. U.S. Air Force Space Command, Operation SEEK GUNFIGHTER – Aggressor Space Applications Project Operational Report (Colorado Springs, CO: Falcon AFB, 23 January 1998), p. 24.

61. Ibid, p. 4.

62. Ibid, p. 7-15.

63. "Countering the Threat Posed by Commercial Satellite Imagery (U)", AF/XOI White Paper, 15 March 1999, p. 13.

64. Newman, Richard J., "The New Space Race, The Pentagon envisions a war in the heavens but can it defend the ultimate high ground?" *U.S. News and World Report*, November 8, 1999, p. 30.

65. Kalish, David E., "Your Secret E-Mail Service," Dec 13, 1999, ABC News. See also http://more.abcnews.go.com/sections/tech/dailynews/internetsecrecy991213.html.

66. Columbia University Seminars, Media and Society, Ethics in America: "Under Orders, Under Fire, p. 4.

67. *Gulf War Air Power Survey Summary Report*, Department of Military Studies, Air University, Maxwell AFB, AL, p. 67, p. 69.

68. Toffler and Toffler, *War and Anti War: Survival at the Dawn of the 21st Century,* Little Brown and Company, 1993, p. 67

69. *Gulf War Air Power Survey Summary Report*, Department of Military Studies, Air University, Maxwell AFB, AL, p. 67 p. 251.

70. Cooper, Jeffrey, "*Another View of the Revolution in Military Affairs*," Strategic Studies Institute, U.S. Army War College, 15 July 1994.

71. Grundhauser, Larry K. "Sentinels Rising", *Airpower Journal*, Winter 98, Vol. 12 Issue 4, p. 67.

72. Builder, Carl H., *The Icarcus Syndrome*, Transaction Publishers, New Brunswick, p. 249.

73. Cooper, Jeffrey R., *Another View of the Revolution in Military Affairs,* 15 July 1994, p. 45.

74. Joint Publication 1

75. Barwinczak, Patricia M. "Achieving Information Superiority," *Military Review*, Sep-Nov 98, Vol. 78, Issue 5, p. 36.

76. Air Force Doctrine Document 2, *Organization and Employment of Aerospace Power*, Spring 99 revision, version 5, pp. 11. (574 blue book)

77. *Air Force Manual 1-1*, Chapter 2, p. 13.

78. Ibid, p. 17.

79. Record, Jeffery, *Ready for What and Modernizing Against Whom?* Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, April 1995, p.7.

80. Tilford, Earl H., *The Revolution in Military Affairs: Prospects and Cautions*, Strategic Studies Institute, U.S. Army War College, 23 June 1995, p. 15.

81. Ibid, p. 15.

82. *Air Force Manual 1-1,* Chapter 2, p. 16.

83 Chandler, Robert W., *The New Faces of War*, p. 231.

84. Ibid, p. 242.

85. Infield, Glen B., *Disaster at Bari*. New York: Macmillan, 1971.

86. Rolfsen, Bruce, "Report: Bases near Combat Zones may be Threatened*", Air Force Times*, November 29, p. 20.

87. *Air Force Manual 1-1*, Chapter 2, p. 20.

88. *Field Manual 100-5, Operations*, May 1986, p. 7-1.

89. *Air Force Manual 1-1*, Chapter 2, p. 17.

90. Estes, Howard (Retired Gen, USSPACECOM), Testimony 1998. www.spacecom.af.mil/usspace/testim98.htm

91. *Gulf War Air Power Survey Summary Report*, Department of Military Studies, Air University, Maxwell AFB, AL, p. 67, p. 248

92. *Air Force Manual 1-1*, Chapter 2, p. 18.

93. As quoted in Dr. Andrew F. Krepinevich, Jr., Testimony Before the Airland Subcommittee, Senate Armed Services Committee on the Future of Tactical Aviation (Washington, D.C.: Center for Strategic and Budgetary Assessments, March 5, 1997), p. 4. (Chandler, pp11)

94. *South China Morning Post*, "Spy Satellites said to Track U.S. Warships", Oct 6, 1999.

95. Ibid.

96. Opall, Barbara, "China Sinks U.S. in Simulated War," *Defense News*, February 5, 1995, p. 1

97. Friedman, George and Meredith, *The Future of War*, Crown Publishers Inc., New York, p. 303.

98. Air Force Research Laboratory engineers and technicians, working in what is now the new aggressor squadron's Space Electronic Warfare Flight, demonstrated how easily it is to build a mobile ultra-high frequency noise source capable of disrupting satellite links. They purchased a Honda electronic generator, copper tubing, PVC pipe from a local home-supply store and electronic components at a swap meet. They assembled these into a noise source, wrote a bit of software code to control it, mounted the system on a pickup truck and "had a working jammer." Total cost was $7,500. Aviation Week and Space, Vol. 152, No. 14, April 3, 2000, p. 53.

99. *Air Force Manual 1-1*, Chapter 2, p. 12.

100. *Air Force Manual 1-1*, Chapter 2, p. 18.

101. Roland, Alex, *The Technological Fix: Weapons and the Cost of War*, Strategic Studies Institute, U.S. Army War College, 6 June 1995, p. iii.

102. Howard, Sir Michael, *How Much Can Technology Change Warfare?* Strategic Studies Institute, U.S. Army War College, 20 July 1994, p. 28.

103. Powell, Colin. "Information-Age Warriors", *Byte*, July 1992, pp. 370.

104. Silkett, Wayne A., "Alliance and Coalition Warfare," *Parameters,* Vol. 23, Summer 93, p. 74.

105. *A National Security Strategy for a Global Age, December 2000,*Washington DC, 65 pp.

106. Hammond, Grant T., "Myths of the Gulf War: Some "Lessons" Not to Learn", *Airpower Journal*, Vol. XII, No., 3, Fall 1998, p. 18.

107. Ibid.

108. Garamone, Jim, "Robertson Calls for NATO to do More," http://www.defenselink.mil/news/Feb2000/n02082000_20002081.html

109. Sands, David R., "Bid to Create EU Army Stalled," *The Washington Times*, January 9, 2000, p. C11. Specifically, the U.S. spent $252.4 billion last year, in 1997 dollars, compared to $140.4 billion spent by the 16 members of European members of NATO combined.

110. There are 750 defense contractors in Europe compared to less than 250 in the U.S. Research and development funding in the U.S. is doled out more effectively to a smaller, more efficient group of contractors. Ibid.

111. Secretary of Defense Cohen's speech to the International Institute of Strategic Studies at San Diego, California, 9 Sept 1999, as reported in www.defenselink.mil/ speeches/1999.

112. Schwartzstein, Stuart J.D., "The Information Revolution and National Security, (Center for Strategic and International Studies Washington D.C.), 1996, p.238.

113. *Strategic Assessment 1999: Priorities for a Turbulent World*, National Defense University, p. 266.

114. Col. John Boyd (Retired) conceived of proper strategy as one that disrupted or incapacitated the enemy's ability to cope by forcing him to operate at a tempo beyond his ability to respond effectively. Success favors the side that can observe, orient, decide, and act (OODA) sooner than the enemy. Meilinger, Col Phillip, *The Paths of Heaven: The Evolution of Airpower Theory*, Air University Press, 1997, p. 592.

115 Clausewitz, Carl Von, *On War*, Princeton New Jersey, 1976, p. 87.

116. Silher, Laura, "He won the war. He lost his job." *Talk*, April2000, p. 138.

117. Ibid, p. 139.

118. Borger, Julian, "Cyberwar Could Spare Bombs," *The Guardian*, 5 November 1999, p. 17.

119. Ibid.

120. "Kosovo War Still Raging in Brussels," *Defense Week*, February 7, 2000, p. 3.

121. O'Hanlon, Michael, *Technological Change and the Future of Warfare*, Brookings Institute Press, Washington D.C., 2000, p. 2.

122. Information superiority is based on dominance in three areas: intelligence (with surveillance and reconnaissance support), C4 (command, control, communications, and computers), and information operations. U.S. Joint Chiefs of Staff, "Information Operations," March 1999, p. 1.

123. Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority," *Parameters*, U.S. Army War College Quarterly, Spring 2000, p. 15. See also http://carlisle-www.army.mil/usawc/Parameters/00sprintg/thomas.htm

124. Ibid, p. 15.

125. Unofficial Transcript: USCINCSPACE Testimony Before the Strategic Subcommittee of the Senate Armed Services Committee, 8 March 2000. Official transcript at http://www.senate.gov/~armed services/hearings/2000/f000308.htm

126. Ibid.

127. Cordesman, Anthony, Aviation *Week and Space*, August 23, 1999, p. 30.

128. *Jane's Defense Weekly*, 9 September 1999, p. 13. (Cordesman, p. 76)

129. Friedman, George and Meredith, The Future of War: Power, Technology and World Dominance in the 21st Century, Crown Publishers, New York, p. 319.

130. Ibid, p 320.

131 Global Crossing, http://206.132.184.108/index.asp

132 *Gulf War Air Power Survey Summary Report*, Department of Military Studies, Air University, Maxwell AFB, AL, p. 70.

133 Ibid., p. 67, and Cordesman, Anthony H., *The Lessons and Non-Lessons of the Air and Missile Campaign in Kosovo*, Center for Strategic and International Studies, Sept 29, 1999, p. 120.

134 Biddle, Stephen and Wade P. Hinkle and Michael P. Fischerkeller, "Skill and Technology in Modern Warfare, *Joint Forces Quarterly*, Summer 1999, p. 19.si

135 Chandler, Robert W., *The New Faces of War*, p. 337.

136 Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority," *Parameters*, U.S. Army War College Quarterly, Spring 2000, p. 20. See also http://carlisle-www.army.mil/usawc/Parameters/00sprintg/thomas.htm

137 Grossman, Elaine, "U.S. Commander in Kosovo Sees Low-Tech Threats to High-Tech Warfare," *Inside the Pentagon*, 9 September 1999, p. 1.

138 Admiral Ellis, quoted in Ibid.

139 Rolfsen, Bruce, "Report: Bases near Combat Zones may be Threatened*", Air Force Times*, November 29, p. 20.

140 Air Force Wargaming Institute, *Global Engagement IV After Action Report,* draft received 6 April 2000, p. iv.

141 Schwartzstein, Stuart J.D., "The Information Revolution and National Security, (Center for Strategic and International Studies Washington D.C.), 1996, p.154.

142 Xiaoli, Zhu and Zhao Xiaozhuo, *Mei'E Xin Junshi Geming* (The United States and Russia in the New Military Revolution), Beijing, AMS Press, 1996, p. 40-45.

143 Ibid.

144 The expression is "Si vis pacam, para bellum" is thought to originates from Caesar's 'De Bello Gallico.' See http://omega.cohums.ohio-state.edu/hyper-lists/classics-1/98-10-01/0070.html.

Center for Strategy and Technology

The Center for Strategy and Technology was established at the Air War College in 1996. Its purpose is to engage in long-term strategic thinking about technology and its implications for U.S. national security.

The Center focuses on education, research, and publications that support the integration of technology into national strategy and policy. Its charter is to support faculty and student research, publish research through books, articles, and occasional papers, fund a regular program of guest speakers, host conferences and symposia on these issues, and engage in collaborative research with U.S. and international academic institutions. As an outside funded activity, the Center enjoys the support of institutions in the strategic, scientific, and technological worlds.

An essential part of this program is to establish relationships with organizations in the Air Force as well as other Department of Defense agencies, and identify potential topics for research projects. Research conducted under the auspices of the Center is published as Occasional Papers and disseminated to senior military and political officials, think tanks, educational institutions, and other interested parties. Through these publications, the Center hopes to promote the integration of technology and strategy in support of U.S. national security objectives.

For further information on the Center on Strategy and technology, please contact:

Grant T. Hammond, Director
Theodore C. Hailes, Deputy Director
Air War College
325 Chennault Circle
Maxwell AFB
Montgomery, Alabama 36112
(334) 953-6996/2985 (DSN 493-6996/2985)
Email: grant.hammond@maxwell.af.mil
ted.hailes@maxwell.af.mil

William C. Martel, Occasional Papers Editor
Naval War College
(401) 841-6428 (DSN 948-6428)
Email: martelw@nwc.navy.mil

Titles in the Occasional Papers Series

1
Reachback Operations for Air Campaign Planning and Execution
Scott M. Britten, September 1997

2
Lasers in Space: Technological Options for Enhancing US Military Capabilities
Mark E. Rogers, November 1997

3
Non-Lethal Technologies: Implications for Military Strategy
Joseph Siniscalchi, March 1998

4
Perils of Reasoning by Historical Analogy: Munich, Vietnam, and the American Use of Force Since 1945
Jeffrey Record, March 1998

5
Lasers and Missile Defense: New Concepts for Space-Based and Ground-Based Laser Weapons
William H. Possel, July 1988

6
Weaponization of Space: Understanding Strategic and Technological Inevitables
Thomas D. Bell, January 1999

7
Legal Constraints or Information Warfare
Mark Russell Shulman, March 1999

8
Serbia and Vietnam: A Preliminary Comparison of U.S. Decisions To Use Force
Jeffrey Record, May 1999

9
Airborne and Space-Based Lasers: An Analysis of Technological and Operational Compatibility
Kenneth W. Barker, June 1999

10
Directed Energy and Fleet Defense: Implications for Naval Warfare
William J. McCarthy, February 2000

11
High Power Microwaves: Strategic and Operational Implications for Warfare
Eileen M. Walling, March 2000

12
Reusable Launch Vehicles and Space Operations
John E. Ward, Jr., March 2000

13
Cruise Missiles and Modern War: Strategic and Technological Implications
David J. Nicholls, March 2000

14
Deeply Buried Facilities: Implications for Military Operations
Eric M. Sepp, March 2000

15
Technology and Command: Implications for Military Operations in the Twenty-first Century
William B. McClure, July 2000

16
Unmanned Aerial Vehicles: Implications for Military Operations
David Glade, July 2000

17
Computer Networks and Information Warfare: Implications for Military Operations
David J. Gruber, July 2000

18
Failed States and Casualty Phobia
Implications for Force Structure and Technology Choices
Jeffrey Record, December 2000

19
War as We Knew It: It Real Revolution in Military Affairs/Understanding Paralysis in Military Operations
Jan S. Breemer, December 2000

20
Using Lasers in Space: Laser Orbital Debris Removal and Asteroid Deflection
Jonathan W. Campbell, December 2000

21
Weapons of Strategic Effect: How Important is Technology?
Colin S. Gray, January 2001

22
U.S. Army Apache Helicopters and U.S. Air Force Expeditionary Forces: Implications for Future Military Operations
Brad Mason, June 2001